

Table 2
Intercept Orders Issued by Judges During Calendar Year 2004

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|--|----------------------------|-----------|------------------------|-----------------|--------------|----------------------|------------------------|------------|-----------------------------------|---|-----------|-----------------|---------------|-----------|----------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| TOTAL | 1,710 | 79 | 52 | 25 | 1,633 | 1,341 | 28 | 28 | 69,980 | 83 | 30 | 1,507 | 65 | 22 | 1 | 2 |
| FEDERAL | 730 | 6 | - | 7 | 723 | 500 | 30 | 30 | 30,877 | 14 | 8 | 678 | 16 | 11 | 1 | 2 |
| ARIZONA | | | | | | | | | | | | | | | | |
| MARICOPA | 1 | 1 | - | - | 1 | 2 | 30 | 30 | 84 | - | - | - | 1 | - | - | - |
| PIMA | 1 | - | - | - | 1 | 5 | 30 | 12 | 69 | - | - | - | 1 | - | - | - |
| STATE ATTORNEY GENERAL | 8 | 2 | - | - | 8 | 14 | 30 | 30 | 593 | - | - | 4 | 4 | - | - | - |
| CALIFORNIA | | | | | | | | | | | | | | | | |
| ALAMEDA | 3 | - | - | - | 3 | 1 | 30 | 30 | 102 | - | - | 3 | - | - | - | - |
| FRESNO | 1 | - | - | - | 1 | - | 30 | - | 28 | - | - | 1 | - | - | - | - |
| IMPERIAL | 3 | - | - | - | 3 | - | 30 | - | 90 | - | - | 3 | - | - | - | - |
| LOS ANGELES | 95 | - | 5 | - | 90 | 30 | 30 | 30 | 3,106 | - | - | 77 | 18 | - | - | - |
| ORANGE | 20 | - | 12 | - | 8 | 2 | 30 | 30 | 207 | - | - | 19 | 1 | - | - | - |
| RIVERSIDE | 12 | 2 | - | - | 12 | 2 | 30 | 30 | 361 | - | - | 11 | 1 | - | - | - |
| SAN BERNARDINO | 28 | - | - | 1 | 27 | 46 | 30 | 30 | 2,059 | - | - | 24 | 4 | - | - | - |
| SAN DIEGO | 17 | - | - | - | 17 | 6 | 30 | 30 | 526 | - | - | 17 | - | - | - | - |
| TEHAMA | 1 | 1 | - | - | 1 | - | 30 | - | 21 | - | - | 1 | - | - | - | - |
| DELAWARE | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 4 | - | - | - | 4 | - | 16 | - | 58 | - | - | 3 | - | 1 | - | - |
| FLORIDA | | | | | | | | | | | | | | | | |
| 4TH JUDICIAL CIRCUIT (DUVAL) | 14 | 2 | - | - | 14 | 11 | 30 | 30 | 602 | - | - | 14 | - | - | - | - |
| 5TH JUDICIAL CIRCUIT (LAKE/MARION) | 5 | - | - | - | 5 | - | 28 | - | 109 | 1 | - | 4 | - | - | - | - |
| 9TH JUDICIAL CIRCUIT (ORANGE/OSCEOLA) | 1 | - | - | - | 1 | - | 17 | - | 17 | - | - | 1 | - | - | - | - |
| 17TH JUDICIAL CIRCUIT (BROWARD) | 6 | - | - | - | 6 | 11 | 30 | 30 | 458 | 1 | - | 5 | - | - | - | - |
| 18TH JUDICIAL CIRCUIT (BREVARD/SEMINOLE) | 14 | 1 | 1 | - | 13 | 7 | 30 | 30 | 463 | - | - | 14 | - | - | - | - |
| 19TH JUDICIAL CIRCUIT (SAINT LUCIE) | 8 | - | - | 2 | 6 | 2 | 30 | 30 | 208 | 2 | - | 6 | - | - | - | - |
| STATE ATTORNEY GENERAL | 24 | - | 1 | - | 23 | 12 | 30 | 30 | 763 | - | - | 24 | - | - | - | - |
| GEORGIA | | | | | | | | | | | | | | | | |
| AUGUSTA | 2 | - | - | - | 2 | - | 23 | - | 42 | - | - | 2 | - | - | - | - |
| BIBB | 3 | - | - | - | 3 | - | 30 | - | 41 | 1 | - | 2 | - | - | - | - |
| CHATHAM | 3 | - | - | - | 3 | - | 30 | - | 57 | - | - | 3 | - | - | - | - |
| CLAYTON | 2 | - | 2 | - | - | - | 30 | - | - | - | - | 2 | - | - | - | - |
| FULTON | 9 | - | - | - | 9 | - | 30 | - | 151 | - | - | 9 | - | - | - | - |
| GWINNETT | 1 | - | - | 4 | 1 | 30 | 30 | 54 | - | - | 3 | 1 | - | - | - | - |
| HOUSTON | 10 | - | - | 1 | 9 | - | 30 | - | 179 | 2 | - | 8 | - | - | - | - |
| ILLINOIS | | | | | | | | | | | | | | | | |
| CLARK | 1 | - | - | - | 1 | - | 30 | - | 30 | 1 | - | - | - | - | - | - |
| MONROE | 4 | - | - | 3 | 1 | - | 30 | - | 1 | 2 | - | - | 1 | 1 | - | - |
| PIATT | 2 | - | - | - | 2 | - | 16 | - | 3 | - | - | - | 2 | - | - | - |
| WINNEBAGO | 14 | - | - | - | 14 | 1 | 29 | 10 | 95 | 10 | 1 | - | - | 3 | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2004 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|----------------------------------|----------------------------|---------|---------------------------|-----------------|------------|--------------------------|---------------------------|--------------------------------------|---|----------|-----------------|--------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | Number of Extensions | Original Authorization | Extensions | Personal Residence | Business | Portable Device | Combination* | Other | Roving | None Specified |
| MARYLAND | | | | | | | | | | | | | | | |
| BALTIMORE | 20 | - | - | - | 20 | 1 | 26 | 30 | 388 | 1 | - | 19 | - | - | - |
| BALTIMORE CITY | 6 | - | - | - | 6 | 3 | 30 | 30 | 189 | - | - | 6 | - | - | - |
| CARROLL | 4 | - | - | - | 4 | 2 | 30 | 30 | 165 | 1 | - | 3 | - | - | - |
| CECIL | 4 | - | 4 | - | - | 3 | 30 | 30 | - | 2 | - | 2 | - | - | - |
| MASSACHUSETTS | | | | | | | | | | | | | | | |
| ESSEX | 8 | - | - | - | 8 | 11 | 11 | 11 | 202 | - | - | 8 | - | - | - |
| HAMPDEN | 8 | 1 | - | - | 8 | 2 | 15 | 15 | 150 | - | 1 | 7 | - | - | - |
| MIDDLESEX | 6 | - | - | - | 6 | 2 | 15 | 15 | 120 | - | - | 6 | - | - | - |
| SUFFOLK | 1 | - | - | - | 1 | - | 15 | - | 15 | - | - | 1 | - | - | - |
| MINNESOTA | | | | | | | | | | | | | | | |
| CLAY | 1 | - | - | - | 1 | - | 30 | - | 12 | - | - | - | - | 1 | - |
| MISSISSIPPI | | | | | | | | | | | | | | | |
| RANKIN | 2 | - | - | - | 2 | - | 30 | - | 48 | - | - | 2 | - | - | - |
| SIMPSON | 1 | - | - | - | 1 | - | 30 | - | 30 | 1 | - | - | - | - | - |
| NEVADA | | | | | | | | | | | | | | | |
| CLARK | 7 | - | 5 | - | 2 | 7 | 30 | 30 | 85 | 1 | - | 5 | 1 | - | - |
| ELKO | 1 | - | - | - | 1 | - | 3 | - | 3 | - | - | - | - | 1 | - |
| NEW HAMPSHIRE | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 13 | 1 | - | - | 13 | 37 | 10 | 10 | 466 | 1 | - | 12 | - | - | - |
| NEW JERSEY | | | | | | | | | | | | | | | |
| BERGEN | 23 | 1 | - | - | 23 | 28 | 20 | 21 | 988 | - | 2 | 21 | - | - | - |
| BURLINGTON | 2 | - | - | 1 | 1 | - | 15 | - | 1 | - | - | 2 | - | - | - |
| CAMDEN | 5 | - | - | - | 5 | 2 | 30 | 30 | 183 | - | - | 5 | - | - | - |
| GLOUCESTER | 3 | 2 | 3 | - | - | - | 20 | - | - | - | - | 1 | 2 | - | - |
| HUDSON | 10 | - | - | - | 10 | 11 | 20 | 12 | 296 | - | - | 10 | - | - | - |
| MIDDLESEX | 3 | - | 1 | - | 2 | 2 | 20 | 10 | 59 | - | - | 3 | - | - | - |
| PASSAIC | 42 | 2 | - | - | 42 | 10 | 22 | 26 | 909 | - | - | 42 | - | - | - |
| SOMERSET | 5 | - | - | - | 5 | 6 | 20 | 10 | 119 | - | - | 5 | - | - | - |
| STATE ATTORNEY GENERAL | 30 | - | 15 | - | 15 | 7 | 28 | 30 | 329 | - | - | 30 | - | - | - |
| UNION | 21 | 1 | 2 | - | 19 | 18 | 21 | 18 | 551 | - | - | 20 | - | 1 | - |
| NEW YORK | | | | | | | | | | | | | | | |
| ALBANY | 3 | - | - | - | 3 | - | 30 | - | 90 | 2 | - | 1 | - | - | - |
| FRANKLIN | 7 | - | - | - | 7 | 2 | 30 | 30 | 233 | - | 1 | 6 | - | - | - |
| HERKIMER | 3 | 1 | - | - | 3 | 1 | 15 | 18 | 63 | - | 2 | 1 | - | - | - |
| KINGS | 11 | 6 | - | 1 | 10 | 9 | 30 | 30 | 493 | - | 1 | 10 | - | - | - |
| MONROE | 3 | - | - | - | 3 | 4 | 30 | 30 | 146 | 2 | - | 1 | - | - | - |
| MONTGOMERY | 1 | - | 1 | - | - | - | 30 | - | - | - | - | 1 | - | - | - |
| NASSAU | 3 | 1 | - | - | 3 | 9 | 30 | 30 | 307 | - | - | 1 | 2 | - | - |
| NEW YORK | 11 | - | - | - | 11 | 78 | 30 | 28 | 2,132 | 4 | 1 | 6 | - | - | - |
| NY ORGANIZED CRIME TASK FORCE | 18 | 7 | - | - | 18 | 52 | 28 | 30 | 1,764 | - | 2 | 10 | 6 | - | - |
| NYC SPECIAL NARCOTICS BUREAU | 76 | 8 | - | 5 | 71 | 32 | 30 | 30 | 2,351 | 2 | - | 72 | - | 2 | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2004 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Personal Residence | Location Authorized in Original Application | | | | | |
|------------------------|----------------------------|---------|------------------------|-----------------|------------|----------------------|------------------------|------------|-----------------------------------|--------------------|---|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | | Business | Portable Device | Combination** | Other | Roving | None Specified |
| NEW YORK (CONTINUED) | | | | | | | | | | | | | | | | |
| ONEIDA | 6 | 3 | - | - | 6 | 2 | 30 | 30 | 189 | 2 | 1 | 3 | - | - | - | - |
| ORANGE | 2 | - | - | - | 2 | 5 | 30 | 30 | 178 | - | - | - | 2 | - | - | - |
| OSWEGO | 1 | - | - | - | 1 | - | 30 | - | 22 | 1 | - | - | - | - | - | - |
| QUEENS | 136 | 9 | - | 1 | 135 | 194 | 26 | 30 | 8,196 | 16 | 4 | 115 | 1 | - | - | - |
| RICHMOND | 2 | 1 | - | - | 2 | 3 | 30 | 30 | 108 | - | - | 2 | - | - | - | - |
| ROCKLAND | 4 | - | - | - | 4 | 4 | 30 | 30 | 198 | - | - | 4 | - | - | - | - |
| STATE ATTORNEY GENERAL | 1 | - | - | - | 1 | 8 | 30 | 30 | 151 | - | - | 1 | - | - | - | - |
| SUFFOLK | 34 | 6 | - | - | 34 | 31 | 28 | 30 | 1,582 | 7 | 4 | 22 | 1 | - | - | - |
| WESTCHESTER | 25 | 6 | - | 1 | 24 | 39 | 27 | 30 | 1,542 | - | 1 | 24 | - | - | - | - |
| OHIO | | | | | | | | | | | | | | | | |
| WASHINGTON | 1 | - | - | - | 1 | - | 14 | - | 14 | 1 | - | - | - | - | - | - |
| OKLAHOMA | | | | | | | | | | | | | | | | |
| GARFIELD | 1 | 1 | - | - | 1 | - | 30 | - | 24 | 1 | - | - | - | - | - | - |
| LINCOLN | 1 | - | - | - | 1 | 1 | 30 | 30 | 43 | - | - | 1 | - | - | - | - |
| OKLAHOMA | 14 | - | - | - | 14 | 2 | 30 | 30 | 440 | 1 | - | 13 | - | - | - | - |
| PENNSYLVANIA | | | | | | | | | | | | | | | | |
| ALLEGHENY | 8 | - | - | - | 8 | 3 | 23 | 17 | 231 | 1 | - | 7 | - | - | - | - |
| CHESTER | 6 | - | - | 1 | 5 | 1 | 30 | 30 | 97 | - | - | 6 | - | - | - | - |
| MONTGOMERY | 5 | 1 | - | - | 5 | - | 30 | - | 39 | 1 | - | 3 | - | 1 | - | - |
| PIKE | 3 | - | - | 1 | 2 | - | 10 | - | 2 | - | - | 3 | - | - | - | - |
| STATE ATTORNEY GENERAL | 10 | - | - | - | 10 | 2 | 29 | 30 | 269 | 1 | 1 | 8 | - | - | - | - |
| TENNESSEE | | | | | | | | | | | | | | | | |
| DAVIDSON | 36 | 5 | - | - | 36 | 52 | 30 | 30 | 2,228 | - | - | 36 | - | - | - | - |
| WISCONSIN | | | | | | | | | | | | | | | | |
| MILWAUKEE | 2 | - | - | - | 2 | 2 | 30 | 17 | 86 | - | - | 2 | - | - | - | - |

* Based on the number of orders for which intercept devices were installed as reported by the prosecuting official.

** Combination refers to the number of authorized interceptions for which more than one location was reported.

Table 3
Major Offenses for Which Court-Authorized Intercepts Were Granted
Pursuant to 18 U.S.C. 2519
January 1 Through December 31, 2004

| Reporting Jurisdiction | Total | Bribery | Gambling | Homicide and Assault | Kidnapping | Larceny, Theft, and Robbery | Loansharking, Usury, and Extortion | Narcotics | Racketeering | Other |
|---|--------------|-----------|-----------|-------------------------|------------|--------------------------------|---------------------------------------|--------------|--------------|-----------|
| TOTAL | 1,710 | 16 | 90 | 48 | 4 | 39 | 5 | 1,308 | 138 | 62 |
| FEDERAL | 730 | 4 | - | 5 | - | 3 | 1 | 646 | 51 | 20 |
| ARIZONA | | | | | | | | | | |
| MARICOPA | 1 | | | | | | | 1 | | |
| PIMA | 1 | | | | | | | 1 | | |
| STATE ATTORNEY GENERAL | 8 | | | | | | | 4 | | 4 |
| CALIFORNIA | | | | | | | | | | |
| ALAMEDA | 3 | | | | | | | 3 | | |
| FRESNO | 1 | | | | | | | 1 | | |
| IMPERIAL | 3 | | | | | | | 3 | | |
| LOS ANGELES | 95 | | | 17 | 1 | | | 75 | | 2 |
| ORANGE | 20 | | | | | | | 20 | | |
| RIVERSIDE | 12 | | | | | | | 12 | | |
| SAN BERNARDINO | 28 | | | 2 | | | | 26 | | |
| SAN DIEGO | 17 | | | | | | | 15 | | 2 |
| TEHAMA | 1 | | | | | | | 1 | | |
| DELAWARE | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 4 | | | | | | | | 2 | 2 |
| FLORIDA | | | | | | | | | | |
| 4TH JUDICIAL CIRCUIT (DUVAL) | 14 | | | | | | | 12 | 2 | |
| 5TH JUDICIAL CIRCUIT (LAKE/MARION) | 5 | | | | | | 2 | 3 | | |
| 9TH JUDICIAL CIRCUIT (ORANGE/OSCEOLA) | 1 | | | | | | | 1 | | |
| 17TH JUDICIAL CIRCUIT (BROWARD) | 6 | | 6 | | | | | | | |
| 18TH JUDICIAL CIRCUIT (BREVARD/SEMINOLE) | 14 | | | | | | | 14 | | |
| 19TH JUDICIAL CIRCUIT (SAINT LUCIE) | 8 | | | 2 | | | | | 6 | |
| STATE ATTORNEY GENERAL | 24 | | | | | | | 7 | 17 | |
| GEORGIA | | | | | | | | | | |
| AUGUSTA | 2 | | | | | | | 2 | | |
| BIBB | 3 | | | | | | | | 3 | |
| CHATHAM | 3 | | | | | | | 3 | | |
| CLAYTON | 2 | | | | | | | 2 | | |
| FULTON | 9 | | | | | | | | 9 | |
| GWINNETT | 4 | | | 1 | 1 | | | 2 | | |
| HOUSTON | 10 | | | | | | | 10 | | |
| ILLINOIS | | | | | | | | | | |
| CLARK | 1 | | | | | | | 1 | | |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2005

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (In Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|---------------------------------------|----------------------------|-----------|------------------------|-----------------|--------------|----------------------|------------------------|------------|-----------------------------------|---|-----------|-----------------|---------------|-----------|----------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| TOTAL | 1,773 | 62 | 57 | 22 | 1,694 | 1,360 | 28 | 28 | 72,897 | 57 | 21 | 1,610 | 49 | 28 | 8 | - |
| FEDERAL | 625 | 3 | - | 1 | 624 | 461 | 30 | 30 | 28,277 | 15 | 6 | 584 | 14 | 5 | 1 | - |
| ARIZONA | | | | | | | | | | | | | | | | |
| MARICOPA | 4 | 1 | - | - | 4 | 3 | 30 | 30 | 178 | - | - | 3 | 1 | - | - | - |
| STATE ATTORNEY GENERAL | 8 | 2 | - | - | 8 | 8 | 30 | 30 | 391 | - | - | 5 | 3 | - | - | - |
| CALIFORNIA | | | | | | | | | | | | | | | | |
| ALAMEDA | 1 | - | - | - | 1 | - | 30 | - | 26 | - | - | 1 | - | - | - | - |
| FRESNO | 3 | - | - | - | 3 | 1 | 30 | 30 | 82 | - | - | 3 | - | - | - | - |
| LOS ANGELES | 102 | - | 11 | - | 91 | 26 | 30 | 30 | 3,135 | 2 | - | 88 | 12 | - | - | - |
| ORANGE | 32 | - | - | 1 | 31 | - | 30 | - | 851 | - | - | 32 | - | - | - | - |
| PLACER | 2 | - | - | - | 2 | - | 30 | - | 46 | - | - | - | 2 | - | - | - |
| RIVERSIDE | 12 | - | - | - | 12 | 12 | 30 | 30 | 712 | - | - | 12 | - | - | - | - |
| SAN BERNARDINO | 18 | - | - | - | 18 | 2 | 30 | 30 | 570 | - | - | 17 | 1 | - | - | - |
| SAN DIEGO | 62 | - | 1 | - | 61 | 35 | 30 | 28 | 2,360 | - | - | 62 | - | - | - | - |
| SANTA BARBARA | 3 | 1 | - | - | 3 | 2 | 28 | 30 | 140 | - | - | 2 | 1 | - | - | - |
| COLORADO | | | | | | | | | | | | | | | | |
| 2ND JUDICIAL DISTRICT (DENVER) | 1 | - | - | - | 1 | - | 30 | - | 30 | - | - | 1 | - | - | - | - |
| 4TH JUDICIAL DISTRICT (EL PASO) | 11 | - | 3 | - | 8 | 2 | 27 | 30 | 251 | - | - | 10 | 1 | - | - | - |
| CONNECTICUT | | | | | | | | | | | | | | | | |
| NEW HAVEN | 3 | - | - | - | 3 | - | 15 | - | 45 | - | - | 3 | - | - | - | - |
| NEW LONDON | 4 | - | - | - | 4 | 1 | 15 | 15 | 68 | 1 | - | 1 | - | 2 | - | - |
| STATE ATTORNEY GENERAL | 4 | - | - | 2 | 2 | - | 15 | - | 30 | 1 | - | 3 | - | - | - | - |
| WATERBURY | 1 | - | - | - | 1 | 1 | 15 | 15 | 28 | - | - | 1 | - | - | - | - |
| FLORIDA | | | | | | | | | | | | | | | | |
| 4TH JUDICIAL CIRCUIT (DUVAL) | 17 | 1 | - | - | 17 | 11 | 30 | 30 | 676 | - | - | 17 | - | - | - | - |
| 5TH JUDICIAL CIRCUIT (LAKE/MARION) | 1 | - | - | - | 1 | - | 30 | - | 18 | - | - | 1 | - | - | - | - |
| 9TH JUDICIAL CIRCUIT (ORANGE/OSCEOLA) | 2 | 1 | - | - | 2 | 1 | 30 | 30 | 75 | - | - | 1 | 1 | - | - | - |
| 13TH JUDICIAL CIRCUIT (HILLSBOROUGH) | 9 | 1 | - | - | 9 | 2 | 30 | 20 | 275 | - | - | 9 | - | - | - | - |
| 17TH JUDICIAL CIRCUIT (BROWARD) | 8 | - | - | - | 8 | 5 | 30 | 30 | 324 | - | - | 8 | - | - | - | - |
| 19TH JUDICIAL CIRCUIT (SAINT LUCIE) | 3 | 1 | 2 | - | 1 | - | 30 | - | 14 | - | - | 3 | - | - | - | - |
| STATE ATTORNEY GENERAL | 32 | 2 | 2 | - | 30 | 14 | 30 | 30 | 1,143 | - | - | 31 | 1 | - | - | - |
| GEORGIA | | | | | | | | | | | | | | | | |
| AUGUSTA | 1 | - | - | - | 1 | - | 30 | - | 20 | - | - | 1 | - | - | - | - |
| BIBB | 3 | - | - | - | 3 | - | 30 | - | 76 | 1 | - | 2 | - | - | - | - |
| FULTON | 2 | - | - | 1 | 1 | - | 30 | - | 11 | - | - | - | 2 | - | - | - |
| GWINNETT | 7 | - | - | - | 7 | - | 30 | - | 118 | - | - | 6 | 1 | - | - | - |
| HOUSTON | 14 | - | - | 1 | 13 | - | 29 | - | 151 | - | - | 14 | - | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2005 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|---------------------------|----------------------------|---------|---------------------------|-----------------|------------|--------------------------|---------------------------|--------------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | Number of Extensions | Original Authorization | Extensions | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| ILLINOIS | | | | | | | | | | | | | | | |
| CLARK | 1 | - | - | - | 1 | - | 30 | - | 29 | 1 | - | - | - | - | - |
| DUPAGE | 1 | - | - | - | 1 | 1 | 30 | 30 | 43 | - | - | - | 1 | - | - |
| POPE | 1 | - | - | - | 1 | 1 | 30 | 2 | 32 | 1 | - | - | - | - | - |
| MARYLAND | | | | | | | | | | | | | | | |
| BALTIMORE | 5 | - | - | - | 5 | 2 | 30 | 30 | 130 | - | - | 4 | - | 1 | - |
| BALTIMORE CITY | 2 | - | - | - | 2 | - | 30 | - | 39 | 1 | - | 1 | - | - | - |
| CECIL | 10 | - | - | - | 10 | 2 | 30 | 30 | 256 | - | - | 10 | - | - | - |
| HARFORD | 5 | - | - | - | 5 | - | 30 | - | 98 | - | - | 5 | - | - | - |
| STATE ATTORNEY GENERAL | 19 | - | - | - | 19 | 3 | 28 | 30 | 481 | 1 | - | 18 | - | - | - |
| MASSACHUSETTS | | | | | | | | | | | | | | | |
| HAMPSHIRE | 1 | - | - | - | 1 | - | 15 | - | 15 | - | - | 1 | - | - | - |
| MIDDLESEX | 10 | - | - | - | 10 | 9 | 15 | 15 | 249 | 2 | 1 | 7 | - | - | - |
| MINNESOTA | | | | | | | | | | | | | | | |
| HENNEPIN | 2 | - | - | - | 2 | 1 | 30 | 30 | 58 | - | - | 2 | - | - | - |
| MISSISSIPPI | | | | | | | | | | | | | | | |
| FORREST | 1 | - | - | - | 1 | - | 30 | - | 17 | - | - | 1 | - | - | - |
| HINDS | 3 | - | - | - | 3 | - | 30 | - | 55 | - | - | 3 | - | - | - |
| LAMAR | 2 | - | - | - | 2 | - | 30 | - | 40 | - | - | 2 | - | - | - |
| LEFLORE | 1 | - | - | - | 1 | - | 30 | - | 17 | - | - | 1 | - | - | - |
| WASHINGTON | 1 | - | - | - | 1 | 1 | 30 | 30 | 36 | - | - | 1 | - | - | - |
| NEVADA | | | | | | | | | | | | | | | |
| CLARK | 2 | - | - | - | 2 | - | 16 | - | 20 | - | - | 1 | 1 | - | - |
| ELKO | 1 | - | - | - | 1 | - | 3 | - | 3 | - | - | 1 | - | - | - |
| NEW JERSEY | | | | | | | | | | | | | | | |
| ATLANTIC | 2 | - | - | - | 2 | 1 | 20 | 10 | 27 | - | - | 2 | - | - | - |
| BURLINGTON | 4 | - | - | 2 | 2 | - | 20 | - | 2 | 1 | - | 3 | - | - | - |
| CAMDEN | 4 | - | - | 1 | 3 | 1 | 30 | 30 | 87 | - | - | 3 | - | 1 | - |
| CAPE MAY | 2 | - | - | - | 2 | - | 30 | - | 28 | - | - | 2 | - | - | - |
| ESSEX | 5 | - | 3 | - | 2 | - | 26 | - | 31 | - | - | 2 | - | 3 | - |
| GLOUCESTER | 1 | - | - | 1 | - | - | 20 | - | - | - | - | - | 1 | - | - |
| HUDSON | 28 | - | - | - | 28 | 13 | 22 | 15 | 608 | 1 | - | 25 | - | 2 | - |
| MIDDLESEX | 5 | - | - | 1 | 4 | - | 20 | - | 63 | - | - | 3 | - | 2 | - |
| MORRIS | 29 | - | 1 | - | 28 | 19 | 20 | 11 | 692 | 1 | - | 28 | - | - | - |
| PASSAIC | 16 | - | - | - | 16 | 4 | 19 | 28 | 273 | - | - | 16 | - | - | - |
| SALEM | 1 | - | - | - | 1 | 1 | 20 | 10 | 30 | - | - | 1 | - | - | - |
| SOMERSET | 20 | - | - | - | 20 | 28 | 20 | 13 | 483 | 1 | - | 19 | - | - | - |
| STATE ATTORNEY GENERAL | 67 | - | 28 | 1 | 38 | 40 | 27 | 24 | 1,194 | 3 | - | 61 | - | 1 | 2 |
| UNION | 34 | 10 | - | - | 34 | 16 | 24 | 24 | 1,014 | - | - | 29 | - | - | 5 |
| NEW YORK | | | | | | | | | | | | | | | |
| ALBANY | 2 | - | - | - | 2 | - | 30 | - | 58 | - | - | 1 | 1 | - | - |
| DUTCHESS | 3 | - | - | - | 3 | 3 | 30 | 30 | 172 | - | - | 3 | - | - | - |
| FRANKLIN | 7 | 1 | - | - | 7 | 9 | 30 | 30 | 410 | 4 | - | 3 | - | - | - |
| JEFFERSON | 1 | - | - | 1 | - | - | 30 | - | - | - | 1 | - | - | - | - |
| KINGS | 3 | - | - | - | 3 | 10 | 29 | 29 | 374 | - | - | 3 | - | - | - |
| MONTGOMERY | 5 | - | - | 1 | 4 | - | 30 | - | 39 | - | - | 5 | - | - | - |
| NASSAU | 7 | 3 | - | - | 7 | 5 | 30 | 30 | 266 | - | - | 7 | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2005 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (In Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|----------------------------------|----------------------------|---------|---------------------------|-----------------|------------|-------------------------|---------------------------|------------|--------------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| NEW YORK (CONTINUED) | | | | | | | | | | | | | | | | |
| NEW YORK | 4 | 1 | 2 | - | 2 | 5 | 30 | 30 | 183 | - | - | 3 | - | 1 | - | - |
| NY ORGANIZED CRIME TASK FORCE | 9 | 3 | - | - | 9 | 36 | 30 | 30 | 1,109 | - | - | 4 | 5 | - | - | - |
| NYC SPECIAL NARCOTICS BUREAU | 148 | 7 | - | 5 | 143 | 89 | 30 | 30 | 5,461 | 6 | - | 138 | - | 4 | - | - |
| ONEIDA | 4 | - | - | - | 4 | 3 | 20 | 19 | 136 | - | - | 4 | - | - | - | - |
| QUEENS | 118 | 5 | 1 | 1 | 116 | 354 | 26 | 29 | 12,275 | 4 | 2 | 110 | - | 2 | - | - |
| RICHMOND | 4 | - | - | - | 4 | 1 | 30 | 30 | 58 | - | - | 4 | - | - | - | - |
| ROCKLAND | 10 | - | - | - | 10 | 6 | 30 | 30 | 380 | - | - | 10 | - | - | - | - |
| SARATOGA | 1 | - | - | - | 1 | - | 10 | - | 10 | - | - | 1 | - | - | - | - |
| SCHENECTADY | 1 | - | - | - | 1 | 1 | 30 | 21 | 41 | - | - | - | 1 | - | - | - |
| STATE ATTORNEY GENERAL | 1 | 1 | 1 | - | - | 9 | 30 | 23 | - | - | - | 1 | - | - | - | - |
| SUFFOLK | 41 | 11 | - | - | 41 | 29 | 30 | 30 | 1,551 | 1 | 10 | 30 | - | - | - | - |
| WAYNE | 2 | - | - | - | 2 | 1 | 27 | 30 | 71 | - | - | 2 | - | - | - | - |
| WESTCHESTER | 20 | 3 | - | - | 20 | 33 | 25 | 29 | 1,268 | - | - | 20 | - | - | - | - |
| NORTH CAROLINA | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 8 | - | - | - | 8 | 4 | 30 | 15 | 245 | - | - | 8 | - | - | - | - |
| OKLAHOMA | | | | | | | | | | | | | | | | |
| GARFIELD | 2 | - | - | - | 2 | 1 | 30 | 30 | 53 | - | - | 2 | - | - | - | - |
| OKLAHOMA | 5 | - | - | - | 5 | - | 30 | - | 149 | - | - | 5 | - | - | - | - |
| OREGON | | | | | | | | | | | | | | | | |
| LANE | 1 | - | - | - | 1 | - | 5 | - | 1 | - | - | - | - | 1 | - | - |
| MARION | 3 | - | - | - | 3 | - | 30 | - | 45 | - | - | 3 | - | - | - | - |
| MULTNOMAH | 2 | - | - | 1 | 1 | - | 16 | - | 5 | - | 1 | 1 | - | - | - | - |
| PENNSYLVANIA | | | | | | | | | | | | | | | | |
| MCKEAN | 1 | - | - | - | 1 | - | 30 | - | 6 | - | - | - | - | 1 | - | - |
| MONTGOMERY | 5 | - | - | - | 5 | - | 30 | - | 61 | - | - | 5 | - | - | - | - |
| STATE ATTORNEY GENERAL | 41 | - | 1 | - | 40 | 8 | 30 | 30 | 983 | 5 | - | 36 | - | - | - | - |
| RHODE ISLAND | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 3 | 1 | - | - | 3 | 5 | 30 | 30 | 167 | - | - | 3 | - | - | - | - |
| TENNESSEE | | | | | | | | | | | | | | | | |
| DAVIDSON | 20 | - | - | 1 | 19 | 18 | 30 | 30 | 914 | - | - | 19 | - | 1 | - | - |
| SHELBY | 1 | 1 | - | - | 1 | - | 30 | - | 15 | - | - | 1 | - | - | - | - |
| TEXAS | | | | | | | | | | | | | | | | |
| BURLESON | 2 | 1 | - | - | 2 | - | 30 | - | 57 | - | - | 2 | - | - | - | - |
| FORT BEND | 1 | 1 | - | - | 1 | - | 30 | - | 23 | - | - | 1 | - | - | - | - |
| STARR | 1 | - | 1 | - | - | - | 2 | - | - | - | - | 1 | - | - | - | - |
| WISCONSIN | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 5 | - | - | - | 5 | - | 22 | - | 40 | 4 | - | 1 | - | - | - | - |

* Based on the number of orders for which intercept devices were installed as reported by the prosecuting official.

** Combination refers to the number of authorized interceptions for which more than one location was reported.

Table 3
Major Offenses for Which Court-Authorized Intercepts Were Granted
Pursuant to 18 U.S.C. 2519
January 1 Through December 31, 2005

| Reporting Jurisdiction | Total | Bribery | Gambling | Homicide and Assault | Kidnapping | Larceny, Theft, and Robbery | Loansharking, Usury, and Extortion | Narcotics | Racketeering | Other |
|--|--------------|----------|-----------|-------------------------|------------|--------------------------------|---------------------------------------|--------------|--------------|-----------|
| TOTAL | 1,773 | 4 | 42 | 82 | 6 | 16 | 8 | 1,433 | 94 | 88 |
| FEDERAL | 625 | 4 | 1 | 3 | - | 3 | 6 | 521 | 42 | 45 |
| ARIZONA | | | | | | | | | | |
| MARICOPA | 4 | - | - | 1 | - | - | - | 3 | - | - |
| STATE ATTORNEY GENERAL | 8 | - | - | 1 | - | - | - | 1 | 3 | 3 |
| CALIFORNIA | | | | | | | | | | |
| ALAMEDA | 1 | - | - | 1 | - | - | - | - | - | - |
| FRESNO | 3 | - | - | - | - | - | - | 3 | - | - |
| LOS ANGELES | 102 | - | - | 17 | - | - | - | 85 | - | - |
| ORANGE | 32 | - | - | 1 | - | - | - | 30 | - | 1 |
| PLACER | 2 | - | - | 2 | - | - | - | - | - | - |
| RIVERSIDE | 12 | - | - | 1 | - | - | - | 11 | - | - |
| SAN BERNARDINO | 18 | - | - | - | - | - | - | 18 | - | - |
| SAN DIEGO | 62 | - | - | - | - | - | - | 61 | - | 1 |
| SANTA BARBARA | 3 | - | - | 1 | - | - | - | 2 | - | - |
| COLORADO | | | | | | | | | | |
| 2ND JUDICIAL DISTRICT (DENVER) | 1 | - | - | - | - | - | - | 1 | - | - |
| 4TH JUDICIAL DISTRICT (EL PASO) | 11 | - | - | 1 | 1 | - | - | 9 | - | - |
| CONNECTICUT | | | | | | | | | | |
| NEW HAVEN | 3 | - | - | - | - | - | - | - | 3 | - |
| NEW LONDON | 4 | - | - | - | - | - | - | - | - | 4 |
| STATE ATTORNEY GENERAL | 4 | - | - | - | - | - | - | - | 4 | - |
| WATERBURY | 1 | - | - | - | - | - | - | 1 | - | - |
| FLORIDA | | | | | | | | | | |
| 4TH JUDICIAL CIRCUIT (DUVAL) | 17 | - | - | - | - | - | - | 17 | - | - |
| 5TH JUDICIAL CIRCUIT (LAKE/MARION) | 1 | - | - | - | - | - | - | 1 | - | - |
| 9TH JUDICIAL CIRCUIT (ORANGE/OSCEOLA) | 2 | - | - | - | - | - | - | 2 | - | - |
| 13TH JUDICIAL CIRCUIT (HILLSBOROUGH) | 9 | - | - | - | - | - | - | 7 | 2 | - |
| 17TH JUDICIAL CIRCUIT (BROWARD) | 8 | - | 4 | - | - | 2 | - | 2 | - | - |
| 19TH JUDICIAL CIRCUIT (SAINT LUCIE) | 3 | - | - | 3 | - | - | - | - | - | - |
| STATE ATTORNEY GENERAL | 32 | - | - | 1 | - | - | - | 31 | - | - |
| GEORGIA | | | | | | | | | | |
| AUGUSTA | 1 | - | - | - | - | - | - | 1 | - | - |
| BIBB | 3 | - | - | - | - | - | - | 3 | - | - |
| FULTON | 2 | - | - | 2 | - | - | - | - | - | - |
| GWINNETT | 7 | - | - | - | - | - | - | 7 | - | - |
| HOUSTON | 14 | - | - | - | - | - | - | 14 | - | - |
| ILLINOIS | | | | | | | | | | |
| CLARK | 1 | - | - | - | - | - | - | 1 | - | - |
| DUPAGE | 1 | - | - | 1 | - | - | - | - | - | - |
| POPE | 1 | - | - | - | - | - | - | 1 | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2006

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|--|----------------------------|-----------|------------------------|-----------------|--------------|----------------------|------------------------|------------|-----------------------------------|---|-----------|-----------------|---------------|-----------|-----------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| TOTAL | 1,839 | 94 | 96 | 29 | 1,714 | 1,228 | 29 | 29 | 68,380 | 48 | 13 | 1,685 | 53 | 24 | 15 | 1 |
| FEDERAL | 461 | 1 | - | - | 461 | 297 | 30 | 30 | 18,978 | 5 | 2 | 447 | 5 | 1 | 1 | - |
| ARIZONA | | | | | | | | | | | | | | | | |
| MARICOPA | 10 | 1 | - | - | 10 | 8 | 27 | 30 | 376 | - | - | 8 | 2 | - | - | - |
| STATE ATTORNEY GENERAL | 7 | 2 | - | - | 7 | 6 | 30 | 24 | 328 | 1 | - | 5 | 1 | - | - | - |
| CALIFORNIA | | | | | | | | | | | | | | | | |
| ALAMEDA | 1 | - | - | - | 1 | - | 30 | - | 26 | - | - | - | 1 | - | - | - |
| CONTRA COSTA | 5 | 1 | - | - | 5 | 3 | 30 | 30 | 219 | - | - | 5 | - | - | - | - |
| FRESNO | 2 | - | - | - | 2 | - | 30 | - | 27 | 1 | - | 1 | - | - | - | - |
| KINGS COUNTY | 1 | - | - | - | 1 | 1 | 27 | 26 | 53 | - | - | - | 1 | - | - | - |
| LOS ANGELES | 233 | - | 2 | 3 | 228 | 44 | 30 | 30 | 7,378 | - | - | 230 | 3 | - | - | - |
| NAPA | 1 | 1 | - | - | 1 | - | 30 | - | 9 | 1 | - | - | - | - | - | - |
| ORANGE | 32 | - | - | 1 | 31 | 8 | 30 | 30 | 917 | - | - | 30 | 2 | - | - | - |
| RIVERSIDE | 23 | - | - | 1 | 22 | 8 | 30 | 30 | 772 | - | - | 21 | 2 | - | - | - |
| SAN BERNARDINO | 34 | - | - | 1 | 33 | 13 | 30 | 30 | 1,165 | - | - | 31 | 3 | - | - | - |
| SAN DIEGO | 80 | - | - | - | 80 | 68 | 30 | 30 | 3,680 | - | - | 78 | 2 | - | - | - |
| SANTA BARBARA | 2 | 1 | - | - | 2 | 1 | 30 | 30 | 82 | - | - | 1 | 1 | - | - | - |
| SANTA CLARA | 1 | - | - | - | 1 | - | 30 | - | 18 | - | - | - | 1 | - | - | - |
| SHASTA | 1 | - | - | - | 1 | - | 30 | - | 19 | - | - | - | 1 | - | - | - |
| STANISLAUS | 3 | - | - | - | 3 | 1 | 30 | 30 | 70 | - | - | 2 | 1 | - | - | - |
| VENTURA | 11 | - | - | - | 11 | 3 | 30 | 30 | 321 | - | - | 6 | 5 | - | - | - |
| COLORADO | | | | | | | | | | | | | | | | |
| 1ST JUDICIAL DISTRICT (JEFFERSON) | 4 | - | - | - | 4 | 4 | 30 | 30 | 240 | - | - | 4 | - | - | - | - |
| 2ND JUDICIAL DISTRICT (DENVER) | 7 | - | - | - | 7 | 2 | 30 | 30 | 217 | - | - | 7 | - | - | - | - |
| 4TH JUDICIAL DISTRICT (EL PASO) | 24 | - | - | 2 | 22 | 1 | 30 | 30 | 642 | 3 | - | 21 | - | - | - | - |
| 21ST JUDICIAL DISTRICT (MESA) | 6 | - | - | - | 6 | 3 | 30 | 30 | 214 | - | - | 6 | - | - | - | - |
| 9TH JUDICIAL DISTRICT (GARFIELD, PITKIN, RIO BLANCO) | 2 | - | - | - | 2 | 2 | 30 | 30 | 111 | - | - | 2 | - | - | - | - |
| CONNECTICUT | | | | | | | | | | | | | | | | |
| NEW HAVEN | 2 | - | - | - | 2 | - | 15 | - | 12 | - | - | 2 | - | - | - | - |
| FLORIDA | | | | | | | | | | | | | | | | |
| 1ST JUDICIAL CIRCUIT (ESCAMBRIA) | 11 | 1 | - | 1 | 10 | 4 | 30 | 30 | 320 | - | - | 11 | - | - | - | - |
| 4TH JUDICIAL CIRCUIT (DUVAL) | 34 | 5 | - | 2 | 32 | 13 | 30 | 30 | 1,096 | - | - | 34 | - | - | - | - |
| 5TH JUDICIAL CIRCUIT (LAKE/MARION) | 3 | - | - | - | 3 | - | 30 | - | 51 | - | - | 3 | - | - | - | - |
| 8TH JUDICIAL CIRCUIT (ALACHUA) | 1 | - | - | - | 1 | - | 30 | - | 23 | - | - | 1 | - | - | - | - |
| 9TH JUDICIAL CIRCUIT (ORANGE/OSCEOLA) | 6 | 2 | - | - | 6 | 1 | 30 | 30 | 161 | - | 1 | 4 | 1 | - | - | - |
| 15TH JUDICIAL CIRCUIT (PALM BEACH) | 3 | - | - | - | 3 | - | 30 | - | 10 | - | - | 3 | - | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2006 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|--|----------------------------|---------|------------------------|-----------------|-----------|----------------------|------------------------|------------|-----------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| FLORIDA (CONTINUED) | | | | | | | | | | | | | | | | |
| 17TH JUDICIAL CIRCUIT (BROWARD) | 4 | - | - | - | 4 | 1 | 30 | 30 | 148 | - | - | 4 | - | - | - | - |
| 18TH JUDICIAL CIRCUIT (BREVARD/SEMINOLE) | 18 | 1 | - | - | 18 | 15 | 30 | 30 | 712 | - | - | 18 | - | - | - | - |
| 19TH JUDICIAL CIRCUIT (SAINT LUCIE) | 8 | 1 | - | - | 8 | 3 | 30 | 30 | 253 | - | - | 8 | - | - | - | - |
| STATE ATTORNEY GENERAL | 10 | 2 | - | - | 10 | 10 | 30 | 22 | 361 | - | - | 9 | - | - | 1 | - |
| GEORGIA | | | | | | | | | | | | | | | | |
| AUGUSTA | 2 | - | - | - | 2 | - | 30 | - | 18 | - | - | 2 | - | - | - | - |
| BARROW | 2 | - | - | - | 2 | - | 30 | - | 29 | - | - | 2 | - | - | - | - |
| BIBB | 2 | - | 2 | - | - | - | 30 | - | - | - | - | 2 | - | - | - | - |
| CHATHAM | 1 | - | - | - | 1 | 1 | 30 | 30 | 33 | - | - | 1 | - | - | - | - |
| GWINNETT | 2 | - | - | - | 2 | - | 30 | - | 10 | - | - | 2 | - | - | - | - |
| HOUSTON | 3 | - | - | - | 3 | 1 | 30 | 30 | 102 | - | - | 3 | - | - | - | - |
| TIFTON | 3 | - | - | - | 3 | 4 | 30 | 30 | 206 | - | - | 3 | - | - | - | - |
| ILLINOIS | | | | | | | | | | | | | | | | |
| DUPAGE | 1 | - | - | - | 1 | - | 30 | - | 3 | - | - | - | - | 1 | - | - |
| KANSAS | | | | | | | | | | | | | | | | |
| SHAWNEE | 1 | 1 | - | - | 1 | - | 30 | - | 28 | - | - | 1 | - | - | - | - |
| MARYLAND | | | | | | | | | | | | | | | | |
| BALTIMORE | 24 | - | - | - | 24 | 8 | 25 | 30 | 628 | 1 | - | 17 | - | - | 6 | - |
| BALTIMORE CITY | 27 | - | 1 | - | 26 | 28 | 29 | 24 | 1,282 | - | - | 26 | - | - | - | 1 |
| CECIL | 2 | - | - | - | 2 | 1 | 30 | 30 | 51 | - | - | 2 | - | - | - | - |
| FREDERICK | 1 | - | - | - | 1 | - | 30 | - | 26 | - | - | 1 | - | - | - | - |
| HARFORD | 4 | - | - | - | 4 | 2 | 30 | 30 | 119 | - | - | 4 | - | - | - | - |
| HOWARD | 2 | - | - | - | 2 | - | 30 | - | 28 | - | - | 2 | - | - | - | - |
| MONTGOMERY | 6 | - | - | - | 6 | 3 | 30 | 30 | 160 | - | - | 6 | - | - | - | - |
| WASHINGTON | 1 | - | - | - | 1 | - | 30 | - | 7 | - | - | 1 | - | - | - | - |
| MASSACHUSETTS | | | | | | | | | | | | | | | | |
| MIDDLESEX | 1 | - | - | - | 1 | - | 15 | - | 10 | - | - | - | 1 | - | - | - |
| NORFOLK | 2 | - | - | - | 2 | - | 15 | - | 1 | - | - | - | - | 2 | - | - |
| STATE ATTORNEY GENERAL | 14 | - | - | - | 14 | 14 | 15 | 15 | 382 | 2 | - | 12 | - | - | - | - |
| NEVADA | | | | | | | | | | | | | | | | |
| CLARK | 8 | - | - | - | 8 | - | 23 | - | 128 | 2 | 1 | 2 | 2 | 1 | - | - |
| ELKO | 2 | - | - | - | 2 | - | 6 | - | 2 | 1 | - | 1 | - | - | - | - |
| NEW JERSEY | | | | | | | | | | | | | | | | |
| ATLANTIC | 1 | - | - | - | 1 | 1 | 20 | 10 | 30 | - | - | 1 | - | - | - | - |
| BERGEN | 16 | - | - | 1 | 15 | 15 | 20 | 10 | 385 | 2 | - | 12 | - | - | 2 | - |
| BURLINGTON | 3 | 3 | - | - | 3 | - | 10 | - | 30 | - | - | 3 | - | - | - | - |
| CAMDEN | 6 | - | - | - | 6 | 1 | 30 | 30 | 182 | - | - | 4 | - | 1 | 1 | - |
| ESSEX | 3 | - | 1 | - | 2 | - | 7 | - | 2 | 2 | - | 1 | - | - | - | - |
| GLOUCESTER | 7 | 7 | 7 | - | - | - | 30 | - | - | - | - | - | - | 7 | - | - |
| HUDSON | 23 | 1 | - | 1 | 22 | 5 | 23 | 10 | 317 | - | - | 21 | - | 1 | 1 | - |
| MERCER | 8 | - | - | - | 8 | 6 | 20 | 10 | 210 | - | - | 8 | - | - | - | - |
| MIDDLESEX | 3 | - | - | - | 3 | - | 18 | - | 40 | - | - | 2 | 1 | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2006 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|--|----------------------------|---------|------------------------|-----------------|------------|----------------------|------------------------|------------|-----------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| NEW JERSEY (CONTINUED) | | | | | | | | | | | | | | | | |
| MORRIS | 13 | - | - | - | 13 | 4 | 22 | 10 | 312 | 1 | - | 10 | - | - | 2 | - |
| PASSAIC | 26 | - | - | - | 26 | 6 | 21 | 17 | 426 | - | - | 26 | - | - | - | - |
| SOMERSET | 15 | - | - | - | 15 | 11 | 20 | 10 | 351 | - | - | 15 | - | - | - | - |
| STATE ATTORNEY GENERAL | 63 | 4 | 45 | - | 18 | 39 | 26 | 27 | 453 | 2 | 2 | 56 | 1 | 1 | 1 | - |
| WARREN | 2 | - | - | - | 2 | 2 | 20 | 10 | 59 | - | - | 2 | - | - | - | - |
| NEW MEXICO | | | | | | | | | | | | | | | | |
| 1ST JUDICIAL DISTRICT (SANTA FE, LOS ALAMOS, RIO ARRIBA) | 1 | - | - | - | 1 | - | 25 | - | 25 | - | - | - | 1 | - | - | - |
| 2ND JUDICIAL DISTRICT (BERNALILLO) | 2 | - | - | - | 2 | - | 30 | - | 30 | - | - | - | 2 | - | - | - |
| NEW YORK | | | | | | | | | | | | | | | | |
| ALBANY | 3 | 2 | - | - | 3 | - | 27 | - | 80 | - | - | 3 | - | - | - | - |
| CHAUTAUQUA | 7 | - | - | - | 7 | 1 | 30 | 14 | 198 | 1 | - | 6 | - | - | - | - |
| DUTCHESS | 7 | - | - | - | 7 | 6 | 30 | 30 | 211 | - | - | 7 | - | - | - | - |
| FULTON | 3 | 1 | - | - | 3 | 1 | 30 | 30 | 109 | - | - | 3 | - | - | - | - |
| KINGS | 23 | 4 | - | - | 23 | 32 | 27 | 29 | 1,363 | 6 | 2 | 15 | - | - | - | - |
| MONROE | 9 | 1 | - | - | 9 | 1 | 30 | 30 | 191 | - | - | 8 | - | 1 | - | - |
| NASSAU | 6 | 5 | - | - | 6 | 5 | 25 | 30 | 252 | - | - | 6 | - | - | - | - |
| NEW YORK | 17 | 3 | - | 2 | 15 | 87 | 30 | 29 | 2,817 | 1 | 2 | 11 | 3 | - | - | - |
| NY ORGANIZED CRIME TASK FORCE | 13 | 6 | - | - | 13 | 30 | 30 | 30 | 934 | - | - | 7 | 6 | - | - | - |
| NYC SPECIAL NARCOTICS BUREAU | 86 | 3 | - | 10 | 76 | 44 | 30 | 30 | 3,127 | 7 | - | 78 | - | 1 | - | - |
| ONEIDA | 1 | 1 | - | - | 1 | 1 | 30 | 30 | 45 | - | - | 1 | - | - | - | - |
| QUEENS | 129 | 4 | - | 3 | 126 | 209 | 27 | 30 | 8,680 | 3 | 2 | 121 | - | 3 | - | - |
| RICHMOND | 3 | - | - | - | 3 | 1 | 30 | 30 | 117 | - | - | 3 | - | - | - | - |
| ROCKLAND | 15 | - | - | 1 | 14 | 15 | 30 | 30 | 755 | - | - | 15 | - | - | - | - |
| SARATOGA | 2 | 1 | - | - | 2 | 3 | 30 | 30 | 96 | - | - | 1 | 1 | - | - | - |
| SCHENECTADY | 3 | 2 | - | - | 3 | 3 | 30 | 30 | 122 | - | - | 2 | 1 | - | - | - |
| STATE ATTORNEY GENERAL | 4 | 3 | - | - | 4 | 19 | 30 | 30 | 516 | - | - | 2 | 2 | - | - | - |
| SUFFOLK | 38 | 14 | 38 | - | - | 46 | 30 | 30 | - | 1 | 1 | 36 | - | - | - | - |
| WESTCHESTER | 8 | 2 | - | - | 8 | 7 | 30 | 30 | 369 | - | - | 8 | - | - | - | - |
| NORTH CAROLINA | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 11 | - | - | - | 11 | 3 | 30 | 30 | 263 | - | - | 11 | - | - | - | - |
| OHIO | | | | | | | | | | | | | | | | |
| FRANKLIN | 11 | 6 | - | - | 11 | 1 | 30 | 30 | 253 | - | - | 11 | - | - | - | - |
| LORAIN | 17 | - | - | - | 17 | 7 | 30 | 30 | 431 | - | - | 17 | - | - | - | - |
| OKLAHOMA | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 7 | - | - | - | 7 | 3 | 30 | 30 | 297 | - | - | 7 | - | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2006 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|-----------------------------------|----------------------------|---------|------------------------|-----------------|------------|----------------------|------------------------|------------|-----------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| OREGON | | | | | | | | | | | | | | | | |
| LANE | 2 | - | - | - | 2 | 1 | 30 | 30 | 17 | 1 | - | - | - | 1 | - | - |
| PENNSYLVANIA | | | | | | | | | | | | | | | | |
| DAUPHIN | 1 | - | - | - | 1 | - | 14 | - | 12 | 1 | - | - | - | - | - | - |
| MONTGOMERY | 11 | - | - | - | 11 | - | 26 | - | 140 | 1 | - | 7 | - | 3 | - | - |
| STATE ATTORNEY GENERAL | 17 | - | - | - | 17 | 6 | 28 | 30 | 561 | 1 | - | 16 | - | - | - | - |
| SOUTH CAROLINA | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 1 | - | - | - | 1 | - | 2 | - | 1 | 1 | - | - | - | - | - | - |
| TENNESSEE | | | | | | | | | | | | | | | | |
| 11TH JUDICIAL CIRCUIT (HAMILTON) | 5 | - | - | - | 5 | 3 | 30 | 30 | 192 | - | - | 5 | - | - | - | - |
| 20TH JUDICIAL DISTRICT (DAVIDSON) | 18 | 1 | - | - | 18 | 17 | 30 | 30 | 847 | - | - | 18 | - | - | - | - |
| 2ND JUDICIAL DISTRICT (SULLIVAN) | 3 | - | - | - | 3 | 3 | 30 | 30 | 180 | - | - | 3 | - | - | - | - |
| TEXAS | | | | | | | | | | | | | | | | |
| HARRIS | 2 | - | - | - | 2 | 1 | 30 | 30 | 47 | - | - | 2 | - | - | - | - |
| WISCONSIN | | | | | | | | | | | | | | | | |
| DANE | 2 | - | - | - | 2 | - | 30 | - | 43 | - | - | 2 | - | - | - | - |

* Based on the number of orders for which intercept devices were installed as reported by the prosecuting official.

** Combination refers to the number of authorized interceptions for which more than one location was reported.

Table 2
Intercept Orders Issued by Judges During Calendar Year 2007

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (In Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|------------------------------------|----------------------------|-----------|------------------------|-----------------|--------------|----------------------|------------------------|------------|-----------------------------------|---|----------|-----------------|---------------|-----------|-----------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| TOTAL | 2,208 | 68 | 56 | 33 | 2,119 | 1,701 | 29 | 29 | 93,117 | 27 | 7 | 2,080 | 36 | 28 | 21 | 9 |
| FEDERAL | 457 | 3 | - | 3 | 454 | 269 | 30 | 30 | 18,643 | 4 | 1 | 445 | 6 | 1 | - | - |
| ARIZONA | | | | | | | | | | | | | | | | |
| MARICOPA | 10 | 3 | - | - | 10 | 9 | 30 | 30 | 490 | - | - | 9 | 1 | - | - | - |
| PIMA | 1 | - | - | - | 1 | - | 30 | - | 1 | - | - | 1 | - | - | - | - |
| STATE ATTORNEY GENERAL | 13 | 3 | - | - | 13 | 11 | 29 | 28 | 542 | - | - | 11 | 2 | - | - | - |
| YUMA | 11 | 1 | 1 | - | 10 | 2 | 30 | 30 | 275 | - | - | 11 | - | - | - | - |
| CALIFORNIA | | | | | | | | | | | | | | | | |
| ALAMEDA | 3 | - | - | - | 3 | - | 30 | - | 46 | - | - | 2 | 1 | - | - | - |
| CONTRA COSTA | 4 | - | - | - | 4 | - | 30 | - | 94 | 1 | - | 3 | - | - | - | - |
| FRESNO | 3 | - | - | - | 3 | 7 | 30 | 30 | 271 | - | - | 3 | - | - | - | - |
| LOS ANGELES | 291 | - | 7 | - | 284 | 110 | 30 | 30 | 10,598 | - | - | 291 | - | - | - | - |
| ORANGE | 1 | - | - | - | 1 | - | 30 | - | 30 | - | - | 1 | - | - | - | - |
| SACRAMENTO | 8 | 1 | - | - | 8 | 2 | 30 | 30 | 221 | - | - | 8 | - | - | - | - |
| SAN BERNARDINO | 61 | - | 2 | - | 59 | 21 | 30 | 30 | 1,948 | - | - | 58 | 3 | - | - | - |
| SAN DIEGO | 132 | - | 1 | - | 131 | 103 | 29 | 30 | 5,638 | 2 | - | 129 | 1 | - | - | - |
| SAN FRANCISCO | 4 | - | - | - | 4 | - | 30 | - | 106 | - | - | 4 | - | - | - | - |
| SAN JOAQUIN | 1 | - | - | - | 1 | 2 | 30 | 30 | 90 | - | - | 1 | - | - | - | - |
| SAN LUIS OBISPO | 4 | - | - | - | 4 | 1 | 30 | 30 | 149 | - | - | 4 | - | - | - | - |
| SAN MATEO | 3 | - | - | - | 3 | - | 26 | - | 54 | - | - | 3 | - | - | - | - |
| SANTA BARBARA | 3 | - | - | - | 3 | - | 30 | - | 58 | - | - | 3 | - | - | - | - |
| SANTA CLARA | 1 | - | - | - | 1 | - | 30 | - | 16 | - | - | 1 | - | - | - | - |
| SOLANO | 1 | - | - | - | 1 | - | 30 | - | 11 | - | - | 1 | - | - | - | - |
| SONOMA | 2 | - | - | - | 2 | - | 24 | - | 49 | - | - | 2 | - | - | - | - |
| STANISLAUS | 9 | - | - | - | 9 | 3 | 30 | 30 | 248 | - | - | 9 | - | - | - | - |
| VENTURA | 29 | - | 1 | - | 28 | 5 | 30 | 28 | 824 | - | - | 26 | 3 | - | - | - |
| COLORADO | | | | | | | | | | | | | | | | |
| 1ST JUDICIAL DISTRICT (JEFFERSON) | 12 | - | - | - | 12 | 7 | 30 | 30 | 508 | - | - | 12 | - | - | - | - |
| 4TH JUDICIAL DISTRICT (EL PASO) | 33 | 1 | - | 3 | 30 | 7 | 29 | 30 | 923 | - | - | 33 | - | - | - | - |
| 10TH JUDICIAL DISTRICT (PUEBLO) | 2 | - | - | - | 2 | - | 30 | - | 58 | - | - | 2 | - | - | - | - |
| 21ST JUDICIAL DISTRICT (MESA) | 3 | - | - | - | 3 | - | 30 | - | 83 | - | - | 3 | - | - | - | - |
| CONNECTICUT | | | | | | | | | | | | | | | | |
| ANSONIA-MILFORD | 3 | 3 | - | - | 3 | - | 15 | - | 45 | - | - | 3 | - | - | - | - |
| HARTFORD | 2 | - | - | - | 2 | - | 15 | - | 30 | - | - | 2 | - | - | - | - |
| STATE ATTORNEY GENERAL | 6 | 6 | - | - | 6 | 9 | 15 | 15 | 222 | - | - | 6 | - | - | - | - |
| FLORIDA | | | | | | | | | | | | | | | | |
| 2ND JUDICIAL CIRCUIT (LEON) | 1 | - | - | - | 1 | - | 30 | - | 25 | - | - | - | 1 | - | - | - |
| 4TH JUDICIAL CIRCUIT (DUVAL) | 20 | - | - | - | 20 | 6 | 30 | 30 | 605 | - | - | 20 | - | - | - | - |
| 5TH JUDICIAL CIRCUIT (LAKE/MARION) | 3 | - | - | - | 3 | 2 | 30 | 30 | 109 | - | - | 3 | - | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2007 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Avg. Length (in Days) | | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|---|----------------------------|---------|---------------------------|-----------------|------------|--------------------------|---------------------------|------------|--------------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | Number of Extensions | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| FLORIDA (CONTINUED) | | | | | | | | | | | | | | | | |
| 7TH JUDICIAL CIRCUIT (VOLUSIA) | 7 | - | - | - | 7 | 2 | 30 | 30 | 204 | - | - | 7 | - | - | - | - |
| 9TH JUDICIAL CIRCUIT (ORANGE/OSCEOLA) | 8 | - | - | 1 | 7 | - | 30 | - | 142 | - | 1 | 7 | - | - | - | - |
| 11TH JUDICIAL CIRCUIT (DADE) | 2 | - | - | - | 2 | - | 30 | - | 51 | - | - | 2 | - | - | - | - |
| 13TH JUDICIAL CIRCUIT (HILLSBOROUGH) | 17 | 2 | - | - | 17 | 6 | 30 | 30 | 519 | - | - | 17 | - | - | - | - |
| 14TH JUDICIAL CIRCUIT (BAY) | 1 | - | - | - | 1 | - | 1 | - | 1 | - | - | - | - | 1 | - | - |
| 15TH JUDICIAL CIRCUIT (PALM BEACH) | 2 | 2 | - | - | 2 | - | 30 | - | 60 | - | - | 2 | - | - | - | - |
| 16TH JUDICIAL CIRCUIT (KEY WEST) | 2 | - | - | - | 2 | 1 | 30 | 30 | 74 | - | - | 2 | - | - | - | - |
| 17TH JUDICIAL CIRCUIT (BROWARD) | 4 | - | - | 1 | 3 | 2 | 30 | 30 | 117 | - | - | 4 | - | - | - | - |
| 18TH JUDICIAL CIRCUIT (BREVARD/SEMINOLE) | 11 | - | - | - | 11 | 2 | 30 | 30 | 275 | - | - | 11 | - | - | - | - |
| 19TH JUDICIAL CIRCUIT (SAINT LUCIE) | 26 | - | - | - | 26 | 6 | 28 | 30 | 708 | - | - | 26 | - | - | - | - |
| GEORGIA | | | | | | | | | | | | | | | | |
| AUGUSTA | 3 | - | - | - | 3 | - | 25 | - | 76 | - | - | 3 | - | - | - | - |
| BIBB | 1 | - | - | - | 1 | - | 30 | - | 29 | - | - | 1 | - | - | - | - |
| COBB | 2 | - | - | - | 2 | 1 | 30 | 30 | 47 | - | 2 | - | - | - | - | - |
| DEKALB | 5 | - | - | - | 5 | 3 | 30 | 30 | 190 | - | - | 5 | - | - | - | - |
| GWINNETT | 17 | 1 | - | - | 17 | 11 | 30 | 30 | 652 | - | - | 15 | 2 | - | - | - |
| IDAHO | | | | | | | | | | | | | | | | |
| CLEARWATER | 1 | - | - | - | 1 | - | 30 | - | - | - | - | - | - | 1 | - | - |
| ILLINOIS | | | | | | | | | | | | | | | | |
| JOHNSON | 1 | - | - | - | 1 | - | 30 | - | 27 | - | - | - | - | - | 1 | - |
| MARYLAND | | | | | | | | | | | | | | | | |
| BALTIMORE | 39 | - | - | - | 39 | 2 | 30 | 30 | 743 | 1 | - | 38 | - | - | - | - |
| BALTIMORE CITY | 42 | 3 | - | - | 42 | 14 | 30 | 28 | 1,140 | - | - | 42 | - | - | - | - |
| FREDERICK | 2 | - | - | - | 2 | - | 30 | - | 60 | - | - | 2 | - | - | - | - |
| HARFORD | 14 | - | - | - | 14 | 10 | 30 | 30 | 470 | - | - | 13 | - | 1 | - | - |
| HOWARD | 10 | 1 | 4 | - | 6 | - | 29 | - | 114 | - | - | 9 | 1 | - | - | - |
| WASHINGTON | 1 | - | - | - | 1 | 1 | 30 | 30 | 48 | - | - | 1 | - | - | - | - |
| MASSACHUSETTS | | | | | | | | | | | | | | | | |
| BRISTOL | 1 | - | - | - | 1 | 1 | 15 | 15 | 28 | - | - | 1 | - | - | - | - |
| MIDDLESEX | 1 | - | - | - | 1 | 1 | 15 | 15 | 30 | - | - | - | 1 | - | - | - |
| NORFOLK | 3 | - | - | - | 3 | 8 | 15 | 15 | 142 | - | - | - | 1 | 2 | - | - |
| SUFFOLK | 4 | - | - | - | 4 | - | 14 | - | 48 | - | 3 | 1 | - | - | - | - |
| MINNESOTA | | | | | | | | | | | | | | | | |
| HENNEPIN | 5 | - | 5 | - | - | 4 | 30 | 30 | - | 3 | - | 2 | - | - | - | - |
| NEVADA | | | | | | | | | | | | | | | | |
| CLARK | 22 | - | - | 1 | 21 | 3 | 29 | 30 | 589 | - | - | 21 | 1 | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2007 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (in Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|------------------------------------|----------------------------|---------|------------------------|-----------------|------------|----------------------|------------------------|------------|-----------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| NEW JERSEY | | | | | | | | | | | | | | | | |
| ATLANTIC | 4 | - | - | - | 4 | 2 | 30 | 30 | 136 | - | - | 4 | - | - | - | - |
| BURLINGTON | 5 | - | - | - | 5 | 1 | 20 | 30 | 67 | - | - | 5 | - | - | - | - |
| CAMDEN | 6 | 2 | - | 1 | 5 | 4 | 30 | 30 | 237 | - | - | - | - | - | 6 | - |
| CAPE MAY | 1 | - | - | - | 1 | 1 | 20 | 10 | 24 | - | - | 1 | - | - | - | - |
| GLOUCESTER | 3 | - | 2 | - | 1 | - | 20 | - | 1 | 1 | - | 2 | - | - | - | - |
| HUDSON | 4 | - | - | - | 4 | - | 20 | - | 75 | - | - | 4 | - | - | - | - |
| HUNTERDON | 1 | - | - | - | 1 | - | 20 | - | 1 | - | - | 1 | - | - | - | - |
| MERCER | 6 | - | - | - | 6 | 4 | 20 | 20 | 144 | - | - | 4 | - | 2 | - | - |
| MIDDLESEX | 3 | - | 2 | - | 1 | - | 17 | - | 19 | - | - | 2 | - | 1 | - | - |
| MONMOUTH | 38 | - | - | 3 | 35 | 22 | 30 | 26 | 1,320 | - | - | 29 | - | - | 9 | - |
| MORRIS | 22 | 2 | - | 4 | 18 | 8 | 23 | 23 | 513 | - | - | 22 | - | - | - | - |
| PASSAIC | 12 | 1 | - | - | 12 | 5 | 20 | 10 | 215 | - | - | 11 | - | - | 1 | - |
| SOMERSET | 26 | - | - | 1 | 25 | 17 | 20 | 10 | 566 | 2 | - | 23 | - | 1 | - | - |
| STATE ATTORNEY GENERAL | 44 | - | 24 | 2 | 18 | 22 | 26 | 26 | 622 | - | - | 38 | 1 | 2 | - | 3 |
| UNION | 25 | 1 | 7 | 1 | 17 | 36 | 30 | 30 | 1,422 | - | - | 20 | - | 2 | 3 | - |
| NEW MEXICO | | | | | | | | | | | | | | | | |
| 2ND JUDICIAL DISTRICT (BERNALILLO) | 3 | - | - | - | 3 | - | 30 | - | 84 | - | - | 2 | 1 | - | - | - |
| NEW YORK | | | | | | | | | | | | | | | | |
| ALBANY | 6 | - | - | - | 6 | 4 | 23 | 10 | 178 | - | - | 6 | - | - | - | - |
| CATTARAUGUS | 1 | - | - | - | 1 | 1 | 30 | 30 | 56 | - | - | 1 | - | - | - | - |
| FRANKLIN | 7 | 4 | - | - | 7 | 4 | 30 | 30 | 290 | 2 | - | 5 | - | - | - | - |
| FULTON | 4 | 2 | - | - | 4 | 1 | 30 | 30 | 113 | - | - | 4 | - | - | - | - |
| MONROE | 7 | - | - | - | 7 | - | 30 | - | 86 | - | - | 5 | - | 2 | - | - |
| MONTGOMERY | 4 | - | - | - | 4 | 4 | 30 | 30 | 137 | - | - | 4 | - | - | - | - |
| NASSAU | 8 | 4 | - | 2 | 6 | 12 | 28 | 30 | 535 | - | - | 5 | 2 | 1 | - | - |
| NEW YORK | 13 | 1 | - | 1 | 12 | 53 | 28 | 28 | 1,794 | - | - | 11 | - | - | - | 2 |
| NIAGARA | 1 | - | - | - | 1 | 1 | 30 | 30 | 60 | - | - | 1 | - | - | - | - |
| NY ORGANIZED CRIME TASK FORCE | 14 | 5 | - | - | 14 | 36 | 30 | 30 | 1,314 | - | - | 10 | 4 | - | - | - |
| NYC SPECIAL NARCOTICS BUREAU | 106 | 7 | - | 3 | 103 | 38 | 30 | 32 | 3,367 | 2 | - | 98 | - | 6 | - | - |
| ONEIDA | 3 | 2 | - | - | 3 | 2 | 30 | 30 | 106 | - | - | 3 | - | - | - | - |
| ONONDAGA | 1 | - | - | - | 1 | 2 | 30 | 30 | 16 | - | - | - | 1 | - | - | - |
| ORANGE | 2 | - | - | - | 2 | 3 | 30 | 30 | 103 | - | - | 1 | 1 | - | - | - |
| QUEENS | 234 | - | - | 5 | 229 | 547 | 28 | 29 | 20,214 | 2 | - | 227 | - | 1 | - | 4 |
| RICHMOND | 2 | 1 | - | - | 2 | 4 | 30 | 30 | 176 | - | - | 2 | - | - | - | - |
| ROCKLAND | 16 | - | - | - | 16 | 8 | 30 | 30 | 681 | - | - | 15 | 1 | - | - | - |
| SARATOGA | 1 | - | - | - | 1 | 2 | 30 | 30 | 88 | - | - | 1 | - | - | - | - |
| SCHENECTADY | 1 | - | - | - | 1 | - | 30 | - | 16 | - | - | - | - | 1 | - | - |
| STATE ATTORNEY GENERAL | 2 | - | - | - | 2 | 28 | 30 | 22 | 644 | - | - | 1 | 1 | - | - | - |
| SUFFOLK | 49 | 2 | - | - | 49 | 70 | 30 | 29 | 2,655 | - | - | 49 | - | - | - | - |
| WAYNE | 8 | - | - | - | 8 | 4 | 30 | 30 | 294 | - | - | 8 | - | - | - | - |
| WESTCHESTER | 28 | 2 | - | - | 28 | 49 | 30 | 30 | 1,950 | 3 | - | 24 | - | 1 | - | - |
| NORTH CAROLINA | | | | | | | | | | | | | | | | |
| COLUMBUS | 1 | - | - | - | 1 | - | 30 | - | 1 | - | - | - | - | 1 | - | - |
| PITT | 1 | - | - | - | 1 | 5 | 30 | 30 | 180 | - | - | 1 | - | - | - | - |
| WAKE | 2 | - | - | - | 2 | 12 | 30 | 30 | 336 | - | - | 2 | - | - | - | - |
| WAYNE | 1 | - | - | - | 1 | 1 | 30 | 30 | 26 | - | - | 1 | - | - | - | - |

Table 2
Intercept Orders Issued by Judges During Calendar Year 2007 (Continued)

| Reporting Jurisdiction | Number of Intercept Orders | | | | | Number of Extensions | Avg. Length (In Days) | | Total Number of Days in Operation | Location Authorized in Original Application | | | | | | |
|-----------------------------------|----------------------------|---------|------------------------|-----------------|------------|----------------------|------------------------|------------|-----------------------------------|---|----------|-----------------|---------------|-------|--------|----------------|
| | Authorized | Amended | No Prosecutor's Report | Never Installed | Installed* | | Original Authorization | Extensions | | Personal Residence | Business | Portable Device | Combination** | Other | Roving | None Specified |
| OHIO | | | | | | | | | | | | | | | | |
| LORAIN | 1 | - | - | - | 1 | - | 30 | - | 25 | 1 | - | - | - | - | - | - |
| MADISON | 1 | - | - | - | 1 | - | 30 | - | 30 | - | - | 1 | - | - | - | - |
| OKLAHOMA | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 4 | - | - | - | 4 | 2 | 24 | 25 | 142 | - | - | 4 | - | - | - | - |
| OREGON | | | | | | | | | | | | | | | | |
| CORVALLIS | 1 | - | - | - | 1 | 1 | 30 | 30 | 60 | - | - | 1 | - | - | - | - |
| LANE | 2 | - | - | - | 2 | 3 | 24 | 30 | 26 | - | - | 1 | - | 1 | - | - |
| PENNSYLVANIA | | | | | | | | | | | | | | | | |
| BUCKS | 1 | 1 | - | - | 1 | - | 30 | - | 22 | - | - | 1 | - | - | - | - |
| DAUPHIN | 23 | 1 | - | - | 23 | 2 | 29 | 30 | 421 | 1 | - | 22 | - | - | - | - |
| LANCASTER | 1 | - | - | - | 1 | - | 30 | - | 5 | - | - | 1 | - | - | - | - |
| MONTGOMERY | 4 | - | - | - | 4 | - | 30 | - | 67 | - | - | 4 | - | - | - | - |
| STATE ATTORNEY GENERAL | 18 | - | - | - | 18 | 6 | 30 | 30 | 531 | 1 | - | 17 | - | - | - | - |
| RHODE ISLAND | | | | | | | | | | | | | | | | |
| STATE ATTORNEY GENERAL | 7 | - | - | - | 7 | 4 | 30 | 30 | 262 | - | - | 7 | - | - | - | - |
| TENNESSEE | | | | | | | | | | | | | | | | |
| 4TH JUDICIAL DISTRICT (SEVIER) | 2 | - | - | - | 2 | - | 30 | - | 41 | 1 | - | - | - | - | 1 | - |
| 9TH JUDICIAL DISTRICT (ROANE) | 1 | - | - | - | 1 | 1 | 30 | 30 | 59 | - | - | 1 | - | - | - | - |
| 20TH JUDICIAL DISTRICT (DAVIDSON) | 17 | - | - | - | 17 | 14 | 30 | 30 | 799 | - | - | 17 | - | - | - | - |
| TEXAS | | | | | | | | | | | | | | | | |
| HARRIS | 4 | - | - | - | 4 | 1 | 30 | 30 | 118 | - | - | 4 | - | - | - | - |
| WISCONSIN | | | | | | | | | | | | | | | | |
| MILWAUKEE | 2 | - | - | - | 2 | - | 30 | - | 45 | - | - | 2 | - | - | - | - |
| WAUPACA | 2 | - | - | 1 | 1 | - | 30 | - | 8 | - | - | 2 | - | - | - | - |

* Based on the number of orders for which intercept devices were installed as reported by the prosecuting official.
** Combination refers to the number of authorized interceptions for which more than one location was reported.

Exhibit D

Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation

Audit Report 08-20
March 2008
Office of the Inspector General

Introduction

Law enforcement agencies use electronic surveillance techniques to acquire evidence for criminal and terrorism investigations. Traditionally, electronic surveillance involved using various techniques to intercept and obtain communication information and content. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) and portions of the Electronic Communications Privacy Act (ECPA) are the primary laws governing the use of electronic surveillance in criminal investigations.¹⁰ Similar rules governing electronic surveillance conducted during foreign intelligence, counterintelligence, and terrorism investigations are found in the Foreign Intelligence Surveillance Act (FISA).¹¹

The rapid pace of technological changes in the way people communicate has presented challenges to law enforcement agencies conducting electronic surveillance for criminal investigations. In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to ensure that the telecommunication industry would build surveillance solutions into the technologies they deploy that allow law enforcement agencies to continue to obtain electronic surveillance information. According to CALEA's assistance capability requirements, telecommunication carriers are to isolate, intercept, and deliver communication content and call identifying information to law enforcement pursuant to lawful authorization.¹²

CALEA Provisions and Responsibilities

CALEA assigned certain responsibilities to the Attorney General, the Federal Communications Commission (FCC), telecommunication carriers, equipment manufacturers (manufacturers), and the Department of Justice (DOJ) Office of the Inspector General (OIG). In February 1995, the Attorney General delegated CALEA management to the Federal Bureau of Investigation (FBI). Table 1 outlines each entity with CALEA responsibilities.

TABLE 1: SUMMARY OF CALEA STATUTORY RESPONSIBILITIES

| Entity | Responsibility |
|--------|---|
| | Ensures industry-wide implementation of the assistance capability requirements. |
| | Consults with state and local law enforcement agencies. |
| | Provides estimates to the telecommunication industry on the number of interceptions that government agencies may need |

12/9/2008

OIG Audit Report 08-20

| | |
|--|--|
| FBI | to conduct. |
| | Establishes rules to facilitate carrier reimbursements. |
| | Allocates appropriated funds to carriers in a manner consistent with law enforcement priorities. |
| | Annually reports to Congress the amount of carrier payments during the preceding year and the projected payments for the current year. |
| FCC | Determines which entities are telecommunication carriers and may exempt any entity or category as a carrier by rulemaking and consulting with the FBI. |
| | Establishes technical standards for compliance with assistance capability requirements if industry associations fail to issue technical standards, or if a government agency or any other person believes that industry-adopted standards are deficient. ¹³ |
| | Reviews and grants or denies petitions for extensions. |
| Telecommunication Carriers and Other Service Providers ¹⁴ | Ensure that equipment, facilities, or services that provide customers the ability to originate, terminate, or direct communications meet the CALEA assistance capability requirements. |
| Equipment Manufacturers | Make available all features or modifications necessary to meet assistance capability requirements, including consulting with carriers over current and planned equipment. |
| OIG ¹⁵ | Report to Congress biennially on the type of equipment, facilities, and services brought into compliance with CALEA and whether costs paid to each carrier for CALEA-required modifications were reasonable and cost effective. |

12/9/2008

OIG Audit Report 08-20

Source: OIG Analysis of CALEA

Effective implementation of CALEA’s provisions is dependant on the joint efforts of government agencies, service providers, and telecommunications equipment manufacturers subject to the law’s requirements.

The Telecommunications Carrier Compliance Fund

CALEA authorized the Attorney General to reimburse telecommunication carriers for modifications made to meet CALEA assistance capability requirements on their equipment, facilities, or services installed or deployed on or before January 1, 1995.¹⁶ In 1996, Congress established the Telecommunications Carrier Compliance Fund (TCCF) and, over subsequent years, appropriated nearly \$500 million for such reimbursements, as shown in Table 2 below.

TABLE 2: DEPOSITS TO THE TELECOMMUNICATIONS CARRIER COMPLIANCE FUND

| Funding Activity | Amount (\$) |
|--|----------------------|
| FY 1997 Direct Appropriations | 60,000,000 |
| FY 1997 Department of Justice Working Capital Fund | 40,000,000 |
| FY 1997 U.S. Postal Inspection Service Transfer | 1,000,000 |
| FY 1997 U.S. Customs Service Transfer | 1,580,270 |
| FY 2000 Direct Appropriations | 15,000,000 |
| FY 2000 Supplemental Appropriations | 181,000,000 |
| FY 2001 Direct Appropriations | 200,976,876 |
| Total TCCF Deposits | \$499,557,146 |

Source: FBI

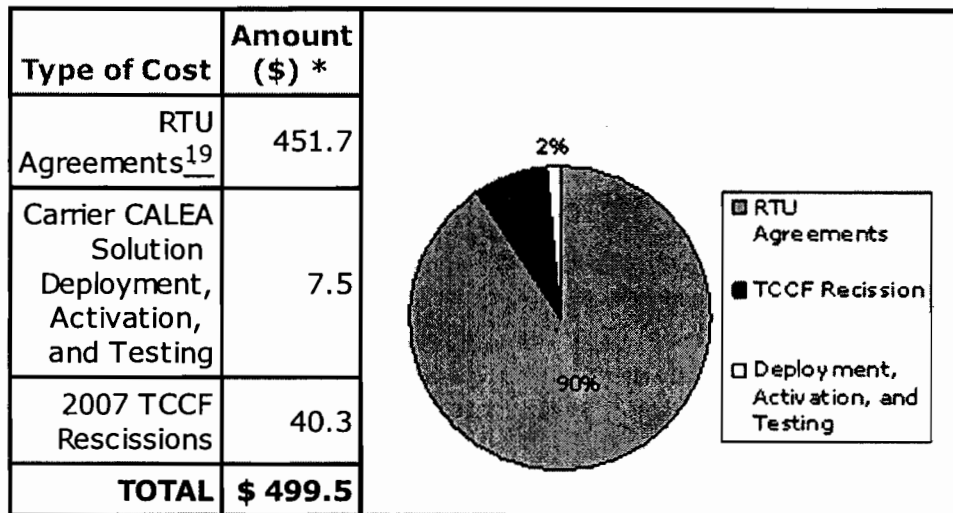
The Attorney General delegated the responsibilities of overseeing the TCCF and compensating carriers for CALEA compliance modifications to the FBI. To carry out these responsibilities, the FBI established a CALEA Implementation Unit (CIU) in its Operational Technology Division and an Offsite Contract Unit (OSCU) in its Finance Division.¹⁷ The CIU worked with carriers, manufacturers, and other telecommunication industry representatives to develop and deploy CALEA-mandated solutions while the OSCU awarded and administered CALEA implementation agreements and audited proposed implementation costs.

In prior OIG audits, we reported on FBI agreements that applied TCCF funds to pay manufacturers for software feature updates and associated licensing fees, referred to as Right-To-Use (RTU) agreements. These payments allowed carriers to obtain CALEA software solutions once the FBI reimbursed development costs to the manufacturer.¹⁸ As shown in the Table 3, the FBI has spent about \$451.7 million on these RTU licenses since 1997.

**TABLE 3: TCCF COST SUMMARY
(1997-2007)**

12/9/2008

OIG Audit Report 08-20



Source: FBI

* Figures in millions, rounded to nearest \$100,000

In addition to the RTU agreements, the FBI spent approximately \$7.5 million to reimburse wire line carriers for deployment, activation, and testing costs of solutions that allow carriers to comply with CALEA requirements, or CALEA solutions. In 2007, Congress rescinded over \$40 million from the TCCF.²⁰ According to a DOJ finance official, the FBI is working with DOJ to transfer the \$5,037 remaining in the TCCF to the DOJ's Working Capital Fund and subsequently close the TCCF account.

Audit Objectives and Scope

The objectives of the audit were to determine: (1) the type of equipment, facilities, and services brought into compliance with CALEA, and (2) whether payments during the most recent 2-year review period for CALEA-required modifications were reasonable and cost effective. In light of the TCCF rescissions that occurred in 2007, our audit also reviewed how the FBI has continued to work with telecommunication providers to help ensure that emerging communication technologies are CALEA compliant.

Our review focused on TCCF-financed activity occurring between January 1, 2006, and December 31, 2007. During the audit, we interviewed officials at FBI Headquarters, the CIU, various FBI Finance Division units, and selected telecommunication providers. We reviewed CALEA annual reports, assessments, associated files, contracts, obligations, and payments for CALEA-implementation.

Footnotes

10. Title III, as amended, contains the procedures law enforcement agencies must follow to obtain the necessary judicial authorization to conduct electronic surveillance, while ECPA, as amended, extends Title III coverage to the contents of electronic messages such as e-mail and to data transmissions from facsimiles and pagers.
11. FISA, as amended, requires carriers to furnish "...all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference..." with the services of the target of electronic surveillance.

12. Call-identifying information is defined as dialed number information that identifies the

12/9/2008

OIG Audit Report 08-20

origin, direction, destination, or termination of any communication generated or received by a subject of surveillance. Content is defined as the substance or meaning of a communication.

13. Electronic surveillance standards provide a basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting electronic surveillance.
14. To meet their responsibilities under CALEA, some carriers have chosen to contract with "trusted third parties." A trusted third party is a private company whose services include providing reviews of a carrier's CALEA-compliance, managing the intercept function, and serving as the custodian of record for the intercept information.
15. See Appendix II for a summary of prior OIG audits.
16. 47 U.S.C. §1008
17. The FBI's Operational Technology Division was formerly called the Investigative Technology Division, while the OSCU was formerly called the Telecommunications Contract and Audit Unit.
18. Our March 2006 report found that the FBI was not provided the cost information necessary to determine the reasonableness of costs associated with RTU agreements. Therefore, the audit offered no opinion on the reasonableness or cost effectiveness of these expenses. See 2006 OIG CALEA Implementation Report, 16.
19. Included in the \$451.7 million figure is a late payment penalty of about \$5,000, for which the FBI could provide no explanation.
20. Pub. L. Nos. 110-5 (2007) and 110-161 (2007).

Exhibit E

11/20/2008

OIG Audit Report 06-13

The Implementation of the Communications Assistance for Law Enforcement Act

Audit Report 06-13
March 2006
Office of the Inspector General

Findings and Recommendations**I. CALEA IMPLEMENTATION COSTS AND PROGRESS**

After 10 years and the expenditure of over \$450 million, the FBI estimates that only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have CALEA software activated and thus are considered CALEA-compliant.⁴⁰ The FBI's strategy for spending these funds focused on identifying switches in locations of high-priority to law enforcement and first ensuring the CALEA-compliance of those switches. While the number of CALEA-compliant switches is based on the best available data, we cannot provide assurance on the accuracy of these estimates. Neither the FBI nor the FCC know the actual percentages of CALEA-compliance because the universe of carriers is unknown. In addition, as reported in previous OIG audits, the cost information provided to us by the FBI did not provide a basis to determine the reasonableness of the costs the FBI incurred.

CALEA Implementation Costs

To facilitate CALEA implementation, Congress authorized the appropriation of \$500 million to reimburse carriers for the direct costs of modifying systems installed or deployed on or before January 1, 1995.⁴¹ In general, costs for achieving compliance for equipment installed after January 1, 1995, were to be incurred by the telecommunications carriers. However, the legislation permitted the FBI, on application of a carrier, to pay that carrier for the additional reasonable costs of making equipment deployed after January 1, 1995, compliant with the assistance capability requirements. However, this applied only if the carrier's compliance could not be reasonably achieved if no payment occurred.

On September 30, 1996, the Omnibus Consolidated Appropriations Act of 1997 amended CALEA by adding Title IV which created the Telecommunications Carrier Compliance Fund (TCCF) and appropriated \$60 million in initial funding. This fund is available without fiscal year limitation to the Attorney General for making payments to telecommunications carriers, equipment manufacturers, and providers of telecommunications support services. Additionally, CALEA authorized agencies with law enforcement and intelligence responsibilities to transfer unobligated balances into the TCCF, subject to applicable congressional reprogramming requirements.

The following table illustrates the dollar amounts and timing of congressional appropriations and fund transfers from authorized agencies with law enforcement and intelligence responsibilities.

| Telecommunications Carrier Compliance Fund Activity | |
|--|----------------------|
| Activity | Amount |
| FY 1997 Direct Appropriations | \$60,000,000 |
| FY 1997 Department of Justice Working Capital Fund | \$40,000,000 |
| FY 1997 U.S. Postal Inspection Service Transfer | \$1,000,000 |
| FY 1997 U.S. Customs Service Transfer | \$1,580,270 |
| FY 2000 Direct Appropriations | \$15,000,000 |
| FY 2000 Supplemental Appropriations | \$181,000,000 |
| FY 2001 Direct Appropriations | \$200,976,876 |
| Total Deposits | \$499,557,146 |

Source: FBI, *Communications Assistance for Law Enforcement Act (CALEA)*
Ninth Annual Report to Congress

Since 1994, the FBI has spent approximately \$450 million to reimburse carriers for their purchase of CALEA-compliant software licenses (referred to throughout this report as Right-to-Use or RTU licenses). The software licensing agreements allowed the software to be installed and activated on both pre- or post-1995 wireline and wireless equipment.⁴²

Right-to-Use (RTU) Software Licenses

An important aspect of the FBI's implementation of CALEA was its nationwide buyout of RTU software licenses. The software allows carriers to meet CALEA intercept requirements by collecting and delivering to law enforcement pertinent call-identifying information, content, or both. The FBI negotiated with carrier and manufacturing representatives to determine the most appropriate way to arrange for carriers to obtain and deploy their CALEA-capability requirements. The FBI concluded that rather than reimbursing each carrier individually for the cost of the RTU licenses, entering into RTU software licenses with equipment manufacturers and their carrier partners would be the best utilization of the appropriated funds. The FBI reasoned that if carriers did not have to pay manufacturers individually for the software licenses, volume discounts could be achieved, thereby reducing deployment costs. This approach allowed carriers to receive, at no charge, CALEA electronic surveillance software.

After extensive negotiations, the FBI entered into several RTU license agreements to reimburse carriers for the purchase of RTU software licenses from certain manufacturers. The agreements were negotiated between February 1998 and April 2003 and allowed carriers to install and activate the CALEA software on either pre-1995 or post-1995 wireline and wireless equipment. By the time these agreements were completed, the FBI had paid approximately \$400 million for the purchase of these licenses from various manufacturers, including Nortel, Lucent, Motorola, Siemens, and AG Communications.⁴³ Through its negotiations, the FBI negotiated substantially reduced costs for the RTU licenses compared to the initial cost proposals as shown in the following chart:

| |
|--------------------------------------|
| Results of RTU Negotiations |
| [Chart Not Available Electronically] |

11/20/2008

OIG Audit Report 06-13

Source: *Determination and Findings Regarding the Implementation of the Communications Assistance for Law Enforcement Act (1999)*

The FBI also entered into additional RTU license agreements, totaling \$50 million, to reimburse carriers for the purchase of RTU Enhanced Dial-Out software licenses from Siemens, Lucent, and Nortel for \$19.8 million, \$19.6 million, and \$10.7 million, respectively.⁴⁴ The FBI determined that these RTU license agreements were the most cost-effective vehicles to reimburse the carriers for the use of the manufacturers' software.

As reported in previous OIG audits (see Appendix V), the cost information given to us by the FBI did not provide a basis to determine the reasonableness of the RTU licenses' costs. Accordingly, we offered no opinion.

Estimates of CALEA-Compliance Progress

After 10 years and the expenditure of over \$450 million, the FBI estimates that only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have the CALEA software activated and thus are considered CALEA-compliant.⁴⁵ The basis of the FBI's estimates on CALEA-compliant switches is its analysis of information provided by carriers that participated in the FBI's flexible deployment initiatives.

The FBI's Flexible Deployment Initiatives

Since 2000, the FBI has offered carriers the opportunity to participate in four flexible deployment initiatives that were designed to provide cost savings and operational flexibility to carriers while ensuring that deployment of CALEA solutions would occur. This approach resulted from recognition by the FBI of the challenges facing carriers and represented an attempt to minimize the costs and operational impact of CALEA-compliance on all carriers.

A carrier's participation in the flexible deployment initiatives allowed it to deploy its CALEA solution in accordance with its normal software upgrade cycle. Under the flexible deployment initiatives, the FBI supported a carrier's petition to the FCC for a time extension for complying with a CALEA deadline if the carrier provided the FBI with its projected CALEA deployment schedules for all switches in its network, as well as information pertaining to any recent electronic surveillance activity. The FBI supported the carriers' projected compliance schedules as long as the schedules did not delay the implementation of CALEA solutions in areas of high priority to law enforcement.⁴⁶ Carrier extensions have become a source of contention between the FBI and telecommunications industry, and this issue is discussed further in the *Carrier Extensions and Enforcement Orders for Non-Compliance* section of Finding II.

The chart below details how the four flexible deployment initiatives the FBI offered carriers addressed different FCC deadlines for CALEA-compliance. In addition, the chart details the number of carriers that filed extensions and the number of switches affected under each flexible deployment initiative:

| Flexible Deployment Initiatives | Type of Technology Addressed | Opening Date to Participate | Closing Date to Participate | Seeking CALEA-Compliance Extension Until | No. of Carriers Filing Extensions | No. of Switches |
|---------------------------------|------------------------------|-----------------------------|-----------------------------|--|-----------------------------------|-----------------|
| FlexD I | wireline/wireless | Jan. 2000 | June 2000 | June 30, 2002 | 1,400 | 10,784 |
| FlexD II | packet-mode | Aug. 2001 | Nov. 2001 | Nov. 19, 2003 | Canceled ⁴⁷ | Canceled |
| FlexD III ⁴⁸ | wireline/wireless | May 2002 | June 2002 | June 30, 2004 | 607 | 7,317 |
| FlexD IV ⁴⁹ | wireline/wireless | May 2004 | June 2004 | June 30, 2006 | 400 | 1,287 |

Source: Federal Bureau of Investigation

The FBI estimated that as of June 2000 about 1,400 carriers filed for 2-year extensions with the FCC under FlexD I. These extensions exempted carriers from complying with CALEA during the 2-year period of the extension. Later, carriers filed for additional time extensions under FlexD III and FlexD IV. As part of FlexD IV, only about 400 carriers – as opposed to the original 1,400 carriers who participated in FlexD I – filed for a time extension with the FCC. Therefore, the FBI concluded that the 1,000 carriers who did not participate in FlexD IV must now be CALEA-compliant since they no longer filed for a time extension.

Further, the FBI used the Local Exchange Routing Guide prepared by the telecommunications industry to estimate the universe of wireline switches for the flexible deployment initiatives. Based on the FBI's review of the Routing Guide, it concluded that 80 to 85 percent of the wireline switches were included in the flexible deployment initiatives. According to the FBI, since all switches must be CALEA-compliant, and the carriers for the remaining 15 to 20 percent of the switches did not petition the FCC for an extension, the FBI concluded that those switches are CALEA-compliant.

As straightforward as this methodology sounds, we cannot provide assurance that it provides an accurate estimate for measuring CALEA compliance. We discussed the extent of CALEA compliance with FCC representatives, who stated that the universe of carriers is unknown, even to the FCC. Telecommunications carriers are licensed by states, not the federal government, and the FCC said that state records are not necessarily up-to-date. Therefore, the universe of carriers may not have been fully represented in the FBI's flexible deployment initiatives. In addition, an accurate estimate of the number of carriers participating in the flexible deployment initiatives is difficult to calculate based on FBI data. In particular, the 400 carriers that participated in FlexD IV were not necessarily a subset of the 1,400 that participated in FlexD I.

According to the FCC, some carriers, like Verizon, indicated that they conducted hundreds of wiretaps for the government and always responded to law enforcement's requests. Other carriers indicated that they never conducted wiretaps even though they were capable of doing so because they did not receive any requests. While CALEA directed carriers to become compliant, it did not require them to substantiate their compliance. Therefore, the FCC did not know if carriers were compliant, or whether they were taking a risk that they would not be called upon to respond to a wiretap request.

Therefore, although we acknowledge that the FBI bases its estimates on the best available data, neither the FBI nor the FCC know the actual percentages of CALEA-compliance because there is no requirement for carriers to report the number of switches that are compliant.

Carrier Information on Compliance

During our interviews with carrier representatives, we requested information regarding the number of switches maintained by the carriers and the CALEA-compliance of those switches.⁵⁰ The five wireline carriers we interviewed provided the following data regarding the CALEA-compliance of their pre- and post-1995 switches:

| Carrier Estimates of CALEA-Compliance for Wireline Switches | | | | | | |
|---|-------------------|------------------------|----------------------------|--------------------|------------------------|----------------------------|
| Carrier | Pre-1995 Switches | Number CALEA-compliant | Percentage CALEA-compliant | Post-1995 Switches | Number CALEA-compliant | Percentage CALEA-compliant |
| Wireline A | 1,900 | 0 | 0% | 300 | 300 | 100% |

11/20/2008

OIG Audit Report 06-13

| | | | | | | |
|------------|-------|-------|--------|-------|-------|------|
| Wireline B | 634 | 634 | 100% | 113 | 113 | 100% |
| Wireline C | - | - | - | *270 | 270 | 100% |
| Wireline D | 1,311 | 989 | 75.44% | 380 | 380 | 100% |
| Wireline E | 290 | 1 | 0.34% | 222 | 222 | 100% |
| TOTAL | 4,135 | 1,624 | 39.27% | 1,285 | 1,285 | 100% |

Source: Carrier representatives
* Wireline C representatives stated that some of its 270 switches may be pre-1995, but, because many of these switches were inherited from other carriers, it is not sure how many.

Specifically, all of the wireline carriers stated that 100 percent of their post-1995 switches were CALEA-compliant, but only one wireline carrier stated that 100 percent of its pre-1995 switches were CALEA-compliant. The other carriers explained that they were awaiting reimbursement from the FBI to begin or complete activation of the CALEA software on their pre-1995 equipment.

We also interviewed representatives from three wireless carriers about the CALEA-compliance of their switches. These carriers maintain only post-1995 switches. All three wireless carriers stated that 100 percent of their switches were CALEA-compliant, as follows:

| Carrier Estimates of CALEA-Compliance for Wireless Switches | | | |
|---|--------------------|------------------------|----------------------------|
| Carrier | Post-1995 Switches | Number CALEA-compliant | Percentage CALEA-compliant |
| Wireless A/B ⁵¹ | 535 | 535 | 100% |
| Wireless F | 174 | 174 | 100% |
| Wireless H | 163 | 163 | 100% |
| TOTAL | 872 | 872 | 100% |

Source: Carrier representatives

Some wireless carriers acknowledged that push-to-talk (PTT) service had been introduced without a CALEA solution and that as a result carriers were unable to perform electronic surveillance in some instances. These carrier officials advised that a PTT CALEA solution had recently been deployed in concert with vendors and law enforcement. The FBI, however, considers this to be an interim solution rather than permanent CALEA solution.

Providers of VoIP service stated that they had not received any request to conduct electronic surveillance on VoIP. One VoIP provider we interviewed was actively developing a CALEA solution. Other carrier representatives stated that an electronic surveillance capability that met both the "J-Standard and punchlist" requirements had been developed for their VoIP services.⁵²

Prior OIG Audit Report

In our April 2004 report, we recommended that the FBI collect and maintain data on the number of carrier switches that are and are not CALEA-compliant. In response to the recommendation, the FBI noted that absent a regulatory or contractual requirement to submit such data, carriers are under no obligation to provide such information. As part of its *Joint Petition*, DOJ requested that the FCC establish rules to permit the FCC to request information regarding CALEA-compliance. As of November 2005, the FCC had not ruled on this issue.

In addition, the FBI developed a carrier survey to collect CALEA-compliance information from carriers on a voluntary basis from carriers. According to the FBI, the information collected in the survey will be used to evaluate the effectiveness of FBI programs for implementing CALEA solutions. Affected telecommunications providers will be asked to identify the extent to which they are CALEA-compliant, or the date when full CALEA-compliance will be achieved if they are not compliant. According to the FBI, the survey was mailed to telecommunications providers during November 2005 and requested responses within 60 days.

Conclusion

The FBI's strategy for spending the \$500 million in CALEA funding focused on identifying switches in locations of high-priority to law enforcement and first ensuring the CALEA-compliance of those switches. According to FBI officials, its CALEA software deployment estimates are based on carrier participation in the FBI's flexible deployment initiatives. However, we cannot provide assurance that the FBI's methodology provides an accurate estimate for measuring compliance because, according to FCC representatives, the universe of carriers is unknown.

The FBI's estimate that only 10 to 20 percent of the wireline switches had the CALEA software activated is troubling because the technology surrounding the PSTN has been used for over 100 years. However, the FBI has encountered significant challenges in implementing CALEA as discussed in Finding II. As a result of the delayed implementation on wireline switches, the law enforcement community may be limited in the type of information it can gather through electronic surveillance. As discussed in Finding III, switches with activated CALEA software have provided federal, state, and local law enforcement with beneficial features to conduct electronic surveillance. However, these features generally have been realized on wireless rather than wireline systems.

II. IMPEDIMENTS TO IMPLEMENTING CALEA

The FBI has encountered significant impediments in implementing CALEA. These impediments included a contentious process of developing technical standards, continuous carrier requests for extensions and enforcement orders for non-compliance, and extended negotiations with carriers over software activation agreements.

Developing Technical Standards

Electronic surveillance standards provide the basis for the development and deployment of technology to permit carriers to assist law enforcement in conducting electronic surveillance. In accordance with CALEA, the FBI consults with carriers and manufacturers to determine what capabilities will be included in the CALEA standards. Developing electronic surveillance standards and obtaining agreement on their content by law enforcement, telecommunications carriers, and equipment manufacturers has been a lengthy process and is the primary reason that CALEA implementation has yet to be completed on wireline equipment.

"Punchlist" Litigation

In June 1996, the FBI issued the Electronic Surveillance Interface (ESI) Document. The ESI set forth law enforcement surveillance capabilities, which

<http://www.usdoj.gov/oig/reports/FB...>

11/20/2008

OIG Audit Report 06-13

were developed in consultation with law enforcement officials and representatives from the telecommunications industry.⁵³

In December 1997, an industry standards-setting group published Interim Standard J-STD-025 (J-Standard) to meet the electronic surveillance capability requirements of CALEA. The J-Standard incorporated many of the requirements set forth in the ESI, but excluded several electronic surveillance capabilities deemed necessary by law enforcement.⁵⁴ As a result, DOJ filed a deficiency petition with the FCC in March 1998 because the J-Standard did not meet the nine capabilities (punchlist) that law enforcement was seeking (see Appendix IV - Public Notice dated April 20, 1998).⁵⁵

In September 1998, the FCC granted an extension to carriers for complying with CALEA capability requirements (see Appendix IV - Memorandum Opinion and Order dated September 10, 1998). For equipment installed or deployed after January 1, 1995, the FCC extended the deadline from October 28, 1998, to June 30, 2000. The FCC granted this extension because no technology available permitted carriers to deploy the minimum industry-developed J-Standard. According to CALEA, carriers are deemed to be CALEA-compliant with respect to equipment installed or deployed on or before January 1, 1995, unless the FBI agrees to reimburse carriers for all reasonable costs necessary to bring such equipment into compliance.

In August 1999, the FCC ruled that carriers must comply with six of the nine punchlist requirements sought by the FBI and not included in the J-Standard (see Appendix IV - Third Report and Order dated August 26, 1999).⁵⁶ The FCC also mandated that carriers provide the capability to intercept packet-mode communications by September 30, 2001. The telecommunications industry appealed the FCC's decision to the U.S. Court of Appeals for the District of Columbia Circuit.

On August 21, 2000, the Court of Appeals remanded four of the challenged punchlist features to the FCC for further proceedings. In an April 11, 2002, Order on Remand, the FCC reiterated its August 1999 decision that all six punchlist capabilities were required under CALEA and must be provided by wireline, wireless, and broadband carriers by June 30, 2002.

Current Standard-Setting Efforts

To ensure that carriers meet their CALEA responsibilities and to promote effective liaison with the telecommunications industry, the FBI participates in several domestic and international standards-setting groups. As part of these groups, the FBI educates carriers and manufacturers about law enforcement's technical assistance capability requirements, and informs the carriers and manufacturers of their CALEA responsibilities with regards to emerging technologies.

The FBI has been, or is currently, involved in several domestic standards-setting groups, including:

| Standards Group | Service Type | Type of Technology |
|--|--------------|---|
| Alliance for Telecommunications Industry Solutions | Voice | Wireline |
| | | Universal Mobile Telecommunications System/General Packet Radio Service |
| | Data Access | Wireline |
| | | Universal Mobile Telecommunications System/General Packet Radio Service |
| Telecommunications Industry Association | Push-to-talk | Universal Mobile Telecommunications System/General Packet Radio Service |
| | | Code Division Multiple Access 2000 |
| | Voice | Wireline/Wireless |
| | | Code Division Multiple Access 2000 |
| American Association of Paging Carriers | Paging | Code Division Multiple Access 2000 |
| | | Code Division Multiple Access 2000 |
| American Mobile Telecommunications Association | Push-to-talk | Traditional Paging, Advanced Messaging, and Ancillary Services |
| | | Enhanced Specialized Mobile Radio |

Source: The Federal Bureau of Investigation

In addition, the FBI has been involved with international standards groups, including the European Telecommunications Standards Institute, the International Softswitch Consortium, and the Third Generation Partnership Project. An FBI official explained that the FBI participates in these groups because many of the equipment manufacturers are based in countries other than the United States. The FBI focuses its involvement in standards groups for technologies in which law enforcement has encountered problems. For example, the FBI does not participate in a standards group addressing satellite telephony because law enforcement has not reported electronic surveillance difficulty with this technology.

Due to the rapid emergence of packet-mode technology and the associated introduction of VoIP and broadband services to the public, the FBI is primarily devoting its resources to setting electronic surveillance standards for packet-mode technologies. As part of this approach, beginning in 2001 the FBI issued three documents setting forth some of law enforcement's needs with regard to electronic surveillance in a packet mode environment: Packet Surveillance Fundamental Needs (PSFN), Carrier Grade Voice over Packet (CGVoP), and Public Internet Protocol Network Access Services (PIPNAS). The PSFN was issued in October 2001 to define the general requirements necessary for the effective delivery of both call-identifying and content data.⁵⁷ The CGVoP was issued in January 2003 to define what call-identifying and content data requirements are needed by law enforcement.⁵⁸ The PIPNAS was issued in September 2003 to set forth law enforcement needs for access to public Internet Protocol (IP) networks and the necessary infrastructure support services.⁵⁹

Work on a packet-mode electronic surveillance standard, J-STD-025B (25B standard) began in October 2001. The 25B standard is only for wireless broadband data access service and was prepared by the Telecommunications Industry Association's (TIA) TR45 Lawfully Authorized Electronic Surveillance Ad Hoc Group. The FBI initially participated in the 25B standard setting effort, but withdrew in February 2003 from active participation in this process. According to FBI officials, their opinion of a proposed standard only counts as one vote at these standard-setting groups, and their contributions to the process were rejected several times. The FBI is considering filing a deficiency petition with the FCC over this standard, as well as for wireline VoIP, wireless VoIP, and wireless broadband access, due to the standards groups' failure to develop a CALEA standard for these technologies that is acceptable to law enforcement. Despite the FBI's belief that the 25B standard is deficient, some carriers we spoke with noted that it is the only official packet-mode standard available and therefore they are upgrading their systems to comply with the 25B standard.

11/20/2008

OIG Audit Report 06-13

Carrier Representatives

Carrier representatives noted the following problems with the standards development process:

- **Slow Vendor Development Time.** According to one carrier, CALEA software solutions development time is generally 18 to 24 months. Therefore, the sooner law enforcement requirements are defined, the sooner CALEA electronic surveillance capabilities can be developed and deployed. Some carrier officials expressed frustration with what they viewed as the slow development of law enforcement requirements. One carrier official stated that the FBI should focus its efforts more on the development of law enforcement requirements and less on the development of ad hoc solutions. An FBI official noted that it is important for the FBI to focus its efforts in both areas because, in some instances, there are no alternative carrier or manufacturer solutions available to conduct the requested electronic surveillance. According to state and local law enforcement officials, the development of ad hoc solutions primarily benefits federal law enforcement because the FBI is not always able to share its technology with state and local law enforcement.⁶⁰ Officials representing a wireless carrier viewed the FBI's development of ad hoc solutions as a hindrance to the development of CALEA solutions because carriers and manufacturers do not always have access to these solutions to understand what hardware and software is needed.
- **Lack of an Adequate Forum.** Carrier officials explained that there was not an adequate forum available for law enforcement, carrier, and manufacturer representatives to meet and discuss mutual concerns. (Law enforcement personnel we interviewed also shared these concerns, which we discuss in Finding IV.) One carrier official noted that carrier and manufacturer's technical staff need to hear law enforcements' concerns firsthand to understand how new technologies impact investigations. The underlying problem often is not understood by the technicians and the result is often that law enforcement needs are viewed as overreaching. Another carrier official stated that current industry standards groups are too technically oriented for law enforcement.
- **Flawed CALEA Solutions.** Carrier officials stated that in the past, manufacturers provided flawed CALEA solutions that a carrier had to fix later at significant expense. Carrier officials suggested that the federal government provide a facility for manufacturers to test CALEA solutions prior to dissemination to carriers.⁶¹ These officials believe that current standard-setting bodies are not good vehicles for this process because they are primarily concerned with standards for commercial applications for the telecommunications industry. Carrier officials said that CALEA is not a high-priority to standard-setting groups and carriers are dependent on the equipment vendors to deliver CALEA-compliant solutions each time a new feature or service is offered. They also stated that only the federal government has the clout to ensure that vendor-developed equipment and software meet CALEA requirements.
- **Acceptance of Standards.** Representatives from one carrier noted that the FBI appears to oppose the acceptance of standards until all of its requirements are accepted, and this ultimately slows progress. According to these representatives, the FBI may benefit more if it progressed slowly through the standards process instead of requesting "everything" in the beginning which some manufacturers and carriers may oppose. For example, one representative stated that the FBI should start with base requirements, get them approved, and then move to addendums that add more requirements and capabilities.

FBI Response to Carriers' Comments

The FBI concurred that the standards development process is slow, and offered comments in the following areas:

- **Industry Controls the Standards-Development Process.** The FBI agreed that the standards development process is slow and contentious. According to the FBI, law enforcement's electronic surveillance needs are known to industry standards groups and only change to reflect the changes made in services offered by providers. For example, law enforcement's need for location information is non-existent in a wireline environment but paramount for a wireless service. As a service provider offers more features, a provider's ability to furnish information regarding those features may need to increase. However, CALEA gives the lead role in setting electronic surveillance standards to the telecommunications industry. This delegation has created considerable tension between the FBI and the telecommunications industry throughout the standards development process. In its CALEA Implementation Plan of August 2003, the FBI discusses providing greater authority to law enforcement for determining technical requirements. According to the FBI, CALEA allows the telecommunications industry to decide what law enforcement needs. If the FBI believes a standard is deficient, it has to challenge the standard by filing a deficiency petition with the FCC. Instead of having to explain why law enforcement needs a particular feature or service, the FBI's preference would be to place the onus on the telecommunications industry to explain why a feature or service that law enforcement wants is not feasible.
 - **Forum for Discussing Law Enforcement Requirements.** The FBI said that the current state of interaction between the telecommunications industry and the FBI is the result of continuous evolution. Over the last decade, various forums have been held regarding the CALEA required capabilities such as telecommunications industry sponsored legal summits, the FBI sponsored Service Specific Document Summits, and conferences and summits held by various organizations (industry and privacy groups). These meetings have allowed participants to express their views – often contentious and contradictory to each other.
 - **Testing CALEA Solutions.** An FBI official believes that the FBI is best suited to test technical solutions from a law enforcement perspective. If, however, the FBI agrees to the carriers' suggestion that it oversee testing, then it is important to define the nature of that testing. Testing for all permutations of the effects of manufacturers' solutions within all providers' networks would impose an enormous burden. Also, it is important to consider how testing is conducted for other services and features made available by equipment manufacturers. For example, large carriers such as Verizon have staffs devoted to extensive testing of the effects of manufacturer-supplied software. For smaller carriers or members of the cable industry, testing has been conducted by the telecommunications industry on a consortium basis. For example, the telecommunications industry often used Telcordia Technologies, Inc. to conduct testing on manufacturer software, and the cable industry used CableLabs to test equipment and software.⁶²
- The FBI stated that the question of adequate testing may best be answered by government-sponsored testing using existing industry mechanisms. For example, FBI-facilitated testing would provide key benefits such as learning how each solution works and the impact solutions have on law-enforcement collection equipment.⁶³ Unfortunately, CALEA does not provide funding for such testing. In addition, the FBI believes that certain legal issues may need to be addressed before such testing could occur. The FBI stated that most carriers test solutions on their own networks or on test networks populated with stored data. In the past, proposals for FBI participation in testing have raised concerns that such participation could be characterized as involving the interception of either real-time or stored communications of a carrier's subscriber. Although not problematic for the carrier who has broad interception authority if necessarily incident to the rendition of a service, there is no statutory exemption in Title III that authorizes law enforcement to conduct, or participate in, intercept testing that involves real-time or stored subscriber communications. Therefore, it is unclear whether a statutory amendment would be required in order to provide the FBI with authority to conduct, or participate in, CALEA testing that involves real-time or stored subscriber communications.
- **Success with Individual Telecommunications Providers.** Although the CALEA standard development process has been slow and contentious, the FBI believes that it has been successful in discussions with individual providers and manufacturers. This is because of the inherent desire on the part of these companies to keep proprietary equipment and network information closely held. For example, an ISP representative noted that his company was launching a VoIP service that was in testing at the time of our audit. According to this representative, his company worked closely with the FBI to ensure that VoIP-CALEA requirements were integrated into its service.

11/20/2008

OIG Audit Report 06-13

Carrier Extensions and Enforcement Orders for Non-Compliance

Two controversial issues regarding CALEA implementation are carrier extensions and enforcement orders for not complying with CALEA.

Carrier Extensions

Under CALEA, the FCC has the power to grant carriers extensions for complying with the CALEA capability requirements. Section 107 of CALEA provides for time extensions for complying with the statute for up to two years if the FCC determines that compliance is not reasonably achievable through available technology. Under Section 109, if the FCC finds that compliance is not reasonably achievable, the Attorney General may, upon petition of the carrier, agree to pay the carrier to make the modifications in order to make compliance reasonably achievable. If the Attorney General does not agree to pay these costs, the carrier will be deemed in compliance with the capability requirements.⁶⁴ Unlike Section 107, there is no maximum time limit on Section 109 extensions. Since June 2000, the FCC has granted hundreds of Section 107 extensions in conjunction with the FBI's flexible deployment initiatives, but never has granted a Section 109 extension.

The Section 107 extensions that were granted to carriers by the FCC are a source of contention between the FBI and the telecommunications industry. According to the FBI, carriers can delay the implementation process by continuing to seek extensions from the FCC. The FCC first issued extensions to wireline and wireless carriers for complying with CALEA until June 30, 2002, and then to June 30, 2004. Furthermore, in 2004 carriers began filing for time extensions for complying with CALEA until June 30, 2006.

Despite the FBI's concerns, carriers argued that extensions were warranted. For example, SBC noted in one of its petitions for an extension that:

In conversations with the FBI, SBC has been led to believe that the FBI will assert that there are no technical reasons why the Siemens Plan C solution cannot be accepted and deployed by SBC. SBC strongly disagrees, and submits that its technical experts are better suited to judge the compatibility of any proposed CALEA solution with SBC's network. It is SBC's understanding that the FBI's opinion is based on testing conducted with a small rural carrier, whose network architecture, personnel, maintenance, and security concerns are vastly different in nature and scope than those faced by SBC. SBC also respectfully suggests that CALEA itself prohibits the FBI or any other government agency from dictating SBC's network architecture, and that forcing adoption of a solution deemed currently unacceptable by SBC's network experts would amount to exactly that.⁶⁵ SBC has worked in good faith with all concerned parties for over a year in an attempt to make the Siemens solution viable for SBC's network, and will continue to do so. Nevertheless, because significant issues remain untested at this time, compliance with CALEA's requirements in SBC's Siemens switches by June 30, 2002 is not reasonably achievable.

A telecommunications industry representative noted that while the FBI blames the FCC for granting carriers repeated extensions, the FBI approached the FCC and suggested the flexible deployment initiatives. He also noted that the extensions were approved in conjunction with the FBI's flexible deployment initiatives, and that an implementation strategy that included hundreds of extensions was "good enough at the time" for the FBI.

In response to the requests for Section 107 extensions, DOJ requested in its *Joint Petition* that the FCC outline criteria for granting both Section 107 and Section 109 extensions for future covered technologies. In response to DOJ's request, the FCC in its Notice of Proposed Rulemaking (NPRM) proposed limiting the availability of time extensions by:

- Restricting the availability of compliance extensions under Section 107, particularly in connection with packet-mode requirements.
- Seeking comments regarding supporting information and documentation that should accompany Section 107 petitions if carriers are not participating in the flexible deployment initiatives, if the FBI opposes the petition of a carrier participating in the program, or if the FBI were to terminate the flexible deployment initiatives.
- Tentatively concluding that the requirements of Section 109 would not be met by a petitioning carrier that merely asserted that CALEA standards had not been developed, or that solutions were not readily available from manufacturers. The FCC noted that if standards or solutions do not exist, the petitioning carriers would still need to demonstrate why they could not negotiate system-specific CALEA solutions with manufacturers or with third-party CALEA service providers.
- Tentatively concluding that carriers may not assert the lack of available standards or solutions to support a showing under Section 109. Instead, carriers filing Section 109 petitions will be expected to demonstrate active and sustained efforts at developing and implementing CALEA solutions for their operations. In addition, the FCC tentatively concluded that it should require Section 109 petitioners to submit detailed information about discussions and negotiations with switch manufacturers, other equipment manufacturers, and third-party CALEA service providers, both before and after the FBI announced the termination of the flexible deployment initiatives in connection with packet-mode technology. Furthermore, the FCC tentatively concluded that unless it was persuaded that petitioners have engaged in sustained and systematic negotiations with manufacturers and third-party providers to design, develop, and implement CALEA solutions, it should reject the submitted petitions.

Enforcement Orders for Non-Compliance

Until this point, the FBI's pursuit of legal remedies for carrier non-compliance with CALEA has not included filing enforcement actions. Under Section 108 of CALEA, an order enforcing CALEA may be issued by the court that approved the electronic surveillance order with which the carrier failed to comply or upon the application of the Attorney General through a civil action. Enforcement orders may only be issued if a court finds that: (1) another carrier's facilities are not reasonably available to conduct the authorized electronic surveillance, and (2) the electronic surveillance is reasonably achievable with available technology.⁶⁶ A court issuing an enforcement order must allow reasonable time for compliance and may impose a civil penalty not to exceed \$10,000 per day for each day of violation of the enforcement order.

The FBI explained that it has not sought enforcement orders for two reasons: (1) pre-1995 equipment is deemed CALEA-compliant until the FBI agrees to reimburse carriers for their deployment costs, and (2) post-1995 equipment has been covered under FCC time extensions that were granted because CALEA-compliance was not reasonably achievable through existing technology. FBI officials summed up the current status by saying that it cannot file suit to enforce CALEA because the carriers currently do not have to comply with the law given the extensions. Instead, the FBI is asking the FCC to use the enforcement powers it has been granted under the Communications Act of 1934 to compel carriers to comply with the FCC-imposed deadlines. According to FBI personnel, the FCC has used these enforcement powers over carriers for other purposes, such as enforcing local number portability and enhanced 911 service.

Telecommunications industry representatives cited law enforcement's failure to file these enforcement actions as evidence that carrier non-compliance is not a concern. Specifically, one industry representative noted that:

[d]espite the crisis atmosphere fostered by the government, the Justice Department and law enforcement have never once used the enforcement powers that CALEA gives them. The only logical conclusion is that there has never been a single case – not one, not anywhere in the country, and not at any time in the last decade – in which the Justice Department thought it could prove that a carrier had failed to meet its CALEA obligation and that important evidence was being lost as a result.

This representative also indicated that carriers were not protected from enforcement action because the FCC had not ruled on the latest extension requests. However, several state and local law enforcement agencies said their failure to file CALEA enforcement actions was a matter of practicality. If

11/20/2008

OIG Audit Report 06-13

they already know a carrier does not have the ability to conduct the electronic surveillance, the agency does not bother going through the trouble and expense of obtaining the court order. In addition, one local law enforcement official noted that although a local judge would be willing to issue an Order to Show Cause against a carrier, the agency would have to wait three months for a hearing. Given that the intercept is needed immediately, the official said the law enforcement agency instead will often pursue a traditional wiretap.⁶⁷

Accordingly, in its *Joint Petition*, DOJ requested that the FCC establish procedures for FCC enforcement actions against entities that do not comply with their CALEA obligations. In the proposed rulemaking, the FCC sought comment from interested parties on how it could enforce the CALEA assistance capability requirements. In addition, the FCC sought comment on whether its general enforcement procedures were sufficient for purposes of CALEA enforcement.

Activation Negotiations on Pre-1995 Equipment

As noted in Finding I, entering into the RTU agreements did not guarantee that CALEA-compliant solutions were made operable and available for use by law enforcement. The agreements only ensured that the RTU licenses for CALEA software were made available to carriers; additional monies are needed to fully deploy the solutions.⁶⁸ While some wireline carriers stated that the RTU software had been activated on pre-1995 equipment in whole or in part, other carriers explained that they were awaiting reimbursement from the FBI to begin or complete activation of the RTU software on their pre-1995 equipment. During mid-2003, the FBI began negotiating reimbursement agreements with four carriers for the cost of deploying CALEA solutions on their pre-1995 equipment.⁶⁹

According to the FBI, it concluded negotiations with two carriers in September 2005 for a total cost of \$4.5 million. The first carrier agreed to the FBI's counter-offer of \$2.9 million to cover 1,158 switches (including dial-out solution software) for an average per switch price of \$2,530. The second carrier agreed to the FBI's counter-offer of \$1.6 million for 667 switches (including dial-out solution software) for an average switch price of \$2,410.

The FBI temporarily discontinued negotiations with the two other carriers. According to the FBI, substantial personnel turnover at the third carrier has made negotiations difficult and discussions were postponed. The negotiation process recently resumed with this carrier. The FBI has also discontinued negotiations with the fourth carrier because they said the carrier's initial proposal of \$170 million appears to be completely unjustified and it far exceeded the amount of the remaining CALEA funding.

Conclusion

The FBI has encountered significant challenges in implementing CALEA. Although new technologies that blur the historical boundaries of telecommunications have emerged, the FBI continues to implement CALEA on wireline systems. The development and implementation of the initial standards, which was slowed significantly by litigation, is the primary reason implementation has been delayed. In addition, repeated requests from carriers for time extensions has been a controversial issue to CALEA implementation. As further discussed in Finding III, the anticipated benefits of CALEA on wireline systems have not materialized.

Recommendation

We recommend that the FBI:

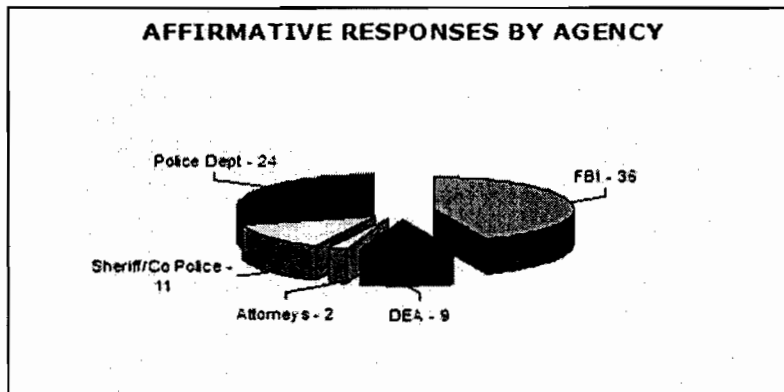
1. Coordinate with the DOJ and the telecommunications industry to determine the legality and feasibility of FBI-sponsored development and testing of manufacturers' CALEA solutions prior to their dissemination to carriers.

III. EFFECTS OF DELAYED CALEA IMPLEMENTATION

CALEA has provided the law enforcement community with beneficial features to conduct electronic surveillance, and has greatly reduced the amount of time it takes to initiate a wiretap. However, these features generally have been realized on wireless rather than wireline systems. Nevertheless, we believe the following factors mitigate the effects of the slow implementation on wireline systems: (1) the growing popularity of Internet telephony, (2) the limited number of wireline intercepts, (3) the apparent limited effect on criminal investigations, and (4) emerging technologies. With the remaining \$45 million in CALEA funding, the FBI plans to reimburse major wireline carriers for activating the CALEA solution software on their systems. However, considering the changing dynamics of the telecommunications industry and the fact that almost 90 percent of intercepts are conducted on wireless systems, we believe the FBI should reexamine the future benefits of activating CALEA software solutions on wireline systems before expending any additional funding in that effort.

Methodology for Measuring CALEA's Impact

We reviewed the FBI's methodology for measuring CALEA's impact and identifying issues and concerns that affect law enforcement's ability to conduct electronic surveillance. In addition, we interviewed federal, state, and local law enforcement officials from five states who had switches that were identified as high-priority by the FBI, and who were provided coverage by a different carrier in each state. We also prepared a written survey that was mailed to 1,396 federal, state, and local law enforcement officials regarding their electronic surveillance activity and use of CALEA features (see Appendix X for a copy of the survey). Of the 723 responses we received to our survey, 82 agencies from 38 states indicated they conduct electronic surveillance. The following chart illustrates the affirmative responses by agency:



Source: Law enforcement responses to the OIG survey

Of the 723 responses received, 641 (89 percent) agencies said they did not conduct electronic surveillance in 2004. The agencies indicated that they

<http://www.usdoj.gov/oig/reports/FB...>

11/20/2008

OIG Audit Report 06-13

did not conduct electronic surveillance for the reasons illustrated below:

| NEGATIVE RESPONSES | | | | | | |
|--------------------|--------------------|--|------------------|---------------------------|---------------------------|-------------------------|
| AGENCY | NEGATIVE RESPONSES | REASON DID NOT CONDUCT ELECTRONIC SURVEILLANCE | | | | |
| | | NOT NECESSARY | COULD NOT AFFORD | CARRIER UNABLE TO CONDUCT | DON'T KNOW HOW TO CONDUCT | OTHER |
| FBI | 0 | 0 | 0 | 0 | 0 | 0 |
| DEA | 0 | 0 | 0 | 0 | 0 | 0 |
| ATTORNEYS | 87 | 80 | 7 | 0 | 11 | 0 |
| SHERIFF/CO POLICE | 107 | 83 | 32 | 1 | 17 | 0 |
| POLICE DEPT | 447 | 363 | 107 | 7 | 65 | 2 (MANPOWER) |
| TOTAL | 641 | 526 | 146 | 8 | 93 | 2 (MANPOWER) |
| % | | 82.06% | 22.78% | 1.25% | 14.51% | 0.31% |

Source: Law enforcement responses to the OIG survey

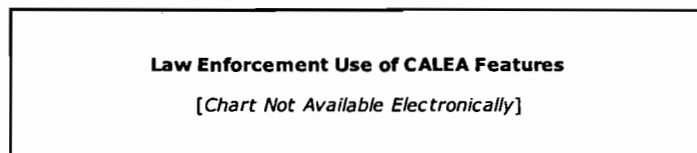
As shown above, FBI and DEA officials responding to the survey indicated that they conducted electronic surveillance in 2004 while responses from 82 percent of the state and local officials indicated that electronic surveillance was not necessary in their cases. Additionally, 23 percent of the state and local agencies responding to the survey indicated that electronic surveillance was not affordable.

Benefits of CALEA

For the switches with activated CALEA software, we found that CALEA has provided federal, state, and local law enforcement with beneficial features to conduct electronic surveillance, and has greatly reduced the amount of time it takes to initiate a wiretap.

CALEA Punchlist Features

As discussed in Finding II, the primary reason for the delayed implementation of CALEA was the litigation over the punchlist features. As noted in Qwest's June 13, 2002, *Petition for Further Extensions of Time of CALEA Deadlines*, the punchlist features represented 5 percent of the capabilities required by law enforcement. We surveyed law enforcement to determine the extent various CALEA features are utilized.⁷⁰ Of the 82 agencies that responded that they performed electronic surveillance, the following chart shows a breakdown of law enforcement's use of the CALEA features:



Source: Law enforcement responses to the OIG survey

Timeliness of Electronic Surveillance

Law enforcement officials stated that CALEA greatly reduced the amount of time it took carriers to initiate a wiretap once a court order was accepted by the carrier. For example, a New York law enforcement official noted that his agency can now initiate a wiretap on a wireless phone within a day. He also said that the carriers have greater capacity to conduct more wiretaps simultaneously. This was reiterated by one carrier official, who noted that prior to deployment of the CALEA solution, provisioning (the providing of electronic surveillance service by the carrier) of electronic surveillance was time-consuming and expensive. In addition, both carrier and law enforcement officials had to be physically present at the switch location during the electronic surveillance, and previously it could take up to several weeks to receive intercept data from a carrier.

With the implementation of CALEA, provisioning is completed remotely from a central location for all electronic surveillance in a carrier's network. This process has significantly reduced carrier and law enforcement travel costs and time, and has facilitated electronic surveillance. Under CALEA, law enforcement agencies can now make a single connection to the carrier's network, and can deal with carrier staff whose positions are dedicated to provisioning electronic surveillance. These changes mean that law enforcement agencies have faster access to electronic surveillance data, often within a day.

Mitigating Factors

We believe the following factors mitigate the effects of the delayed implementation on wireline systems.

Growing Popularity of Internet Telephony

Internet telephony and Internet telephony service providers are a growing segment of the telephone industry. An April 2005 report from research firm International Data Corporation (IDC) predicts that U.S. residential VoIP customers will grow from 3 million in 2005 to 27 million by the end of 2009. An example of this trend is Comcast Corporation, which is the nation's largest cable company. Comcast plans to offer its Internet-based phone service to its 28 million cable and high-speed Internet customers by mid-2006. In addition, a carrier representative we interviewed reiterated a widely held belief that the Internet will swallow up the conventional telephone network, and that Internet Telephony will essentially replace traditional telephone service in the United States in the near future.

Limited Number of Wireline Intercepts

According to the April 2005 *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications*, the most common location specified in wiretap applications authorized in 2004 was "portable device, carried by/on individual."⁷¹ According to the report, 88 percent of all wiretaps authorized involved portable devices such as portable digital pagers and cellular telephones. The report noted that since 2000 – the first year that the "portable device, carried by/on individual" category was used – the proportion of wiretaps involving fixed locations has declined as the use of mobile communications devices has become more

11/20/2008

OIG Audit Report 06-13

prevalent.⁷² The report also noted that only 5 percent of all intercept devices were authorized for personal residences, and 2 percent were authorized for business establishments such as offices, restaurants, and hotels.

In addition, our discussions with four wireline carriers in areas of the country with high amounts of intercept activity revealed that from 2002 to 2004 a limited number of court orders for wiretaps requiring CALEA features were requested:

- Wireline A. 1.2 percent of the court orders it received for intercepts required CALEA features.
- Wireline B. Less than 1 percent of the court orders it received for intercepts required CALEA features.
- Wireline D. 6.25 percent of the court orders it received for intercepts required CALEA features.
- Wireline E. 3.5 percent of the court orders it received for intercepts required CALEA features.

According to the Federal, state, and local law enforcement officials we interviewed and surveyed, their agencies do not request intercepts requiring CALEA features for several reasons (i.e., the high cost charged by carriers, carrier noncompliance, or the investigation only required a traditional wiretap).

The Apparent Limited Effect on Criminal Investigations

The FBI measures the investigative impact of CALEA and identifies issues and concerns of law enforcement in a variety of ways. Representatives from the FBI speak with law enforcement at various events including the FBI's Law Enforcement Technical Forum, the FBI's Law Enforcement Executive Forum, meetings of the International Association of Chiefs of Police, and meetings of the Law Enforcement Executive Development Association.⁷³ During these events, FBI officials said that law enforcement representatives raise with them issues that affect their ability to conduct electronic surveillance, such as carrier compliance and emerging technologies. Federal, state, and local law enforcement representatives also convey their issues and concerns through Threat Assessment Surveys distributed by the FBI.

The FBI also measures the impact of CALEA on law enforcement by reviewing help desk reports. The FBI maintains a help desk that law enforcement officials can call when they have difficulty conducting electronic surveillance or if they have questions. In addition, the FBI website (www.askcalea.net) provides a help desk database that describes difficulties encountered with CALEA solutions. Law enforcement officials can submit problems to the help desk, such as difficulties they encounter while conducting a CALEA intercept. Law enforcement officials can review the help desk's database to determine if other law enforcement agencies have encountered the same difficulty and identify what action was taken.

FBI's Threat Assessment Survey

We reviewed the FBI's 2004 Threat Assessment Survey Report and the individual threat assessment surveys used to prepare the report. The 2004 Threat Assessment Survey was developed to better understand and anticipate future threats to law enforcement. The survey was conducted from November 2003 through September 2004 at the national and regional meetings of the National Technical Investigator Association, and at various DEA and FBI training sessions.

Our review of the surveys found that they are useful in helping the FBI measure CALEA's impact and for identifying issues and concerns that affect law enforcement's ability to conduct electronic surveillance. However, the number of survey participants was limited, and therefore may not adequately represent the full law enforcement community.

The FBI collected 120 surveys from federal, state, and local law enforcement officers from 57 different federal, state, and local agencies and departments. Our review of the surveys revealed that 77 of the 120 participants (64 percent) indicated that criminals have the ability to evade law enforcement's electronic surveillance efforts. Of the 120 participants, 59 participants (49 percent) believed that criminals evaded surveillance using wireless phones, and 50 participants (42 percent) believed the use of the Internet allowed criminal evasion of electronic surveillance. The following chart provides the results of our review:



Source: OIG analysis of 120 FBI Threat Assessment Surveys

We noted that 25 participants (21 percent) believed criminals used telephone company features (call-forwarding, voice mail, 3-way calling) to evade electronic surveillance. However, because the survey responses were general in nature, we were unable to determine the specific features, if any, that were problematic to law enforcement or the extent of the problem. In our judgment, this is a shortcoming in the FBI's survey because it does not identify whether the problem results from a non-CALEA compliant carrier, or the law enforcement agency does not possess the resources to acquire the CALEA features.⁷⁴ For example, two law enforcement officials informed us that their agency cannot afford the expense of installing a T-1 line, which is the delivery method to receive the CALEA features (this issue is discussed further in Finding IV).

The surveys also requested participants to prioritize current, new, or emerging technologies having the greatest impact on their agency's ability to perform electronic surveillance. As shown in the following chart, law enforcement officers indicated that pre-paid cell phones, telephony over broadband, and voice or text over the Internet would have the greatest impact on their department's electronic surveillance activities within the next two years.

Source: OIG analysis of 120 FBI Threat Assessment Surveys

Our review of the FBI's Threat Assessment Surveys revealed that the law enforcement community is less concerned over the ability to perform electronic surveillance on wireline equipment, and more concerned over new and emerging technologies. In addition, we believe the FBI should obtain a larger audience of survey participants to include more state and local law enforcement representatives and provide comprehensive examples of the electronic surveillance problems law enforcement is encountering.

Case Examples

During our audit, we requested specific examples that illustrate existing intercept problems. The FBI provided us with a document entitled *FBI Investigative Technology Division CALEA Law Enforcement Case Examples* dated October 29, 2004. In addition, a DOJ official provided a memorandum, dated March 30, 2005, describing instances where law enforcement has encountered problems with emerging technologies. According to the memorandum, these examples underscore "the importance of addressing vulnerabilities before they have matured into widespread problems that have an irreversible significant detrimental impact on law enforcement and national security interests."

The FBI's document contained a total of 57 case examples representing federal, state, and local law enforcement experiences with CALEA wiretaps. Twenty-seven of the examples described intercepts that were successful, 23 described intercepts that were unsuccessful, and the remaining 8 provided general comments that did not specifically address either a successful or unsuccessful intercept (e.g. information from informants regarding the use of push-to-talk (PTT) and VoIP). None of the examples, however, noted electronic surveillance problems for wireline intercepts. The unsuccessful intercepts were as follows:

11/20/2008

OIG Audit Report 06-13

- Sixteen of the case examples described unsuccessful PTT intercepts, with the most recent example occurring in August 2004.⁷⁵ The carriers cited and the number of instances where law enforcement was unable to conduct electronic surveillance were as follows: [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].
- Three of the case examples described unsuccessful VoIP intercepts. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].
- Two case examples cited pre-paid calling card or pre-paid cell phone for the cause of an unsuccessful intercept. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].
- Two case examples cited carrier issues regarding lack of audio as the cause of an unsuccessful intercept. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

In our judgment, these examples are not necessarily indicative of emerging technology that is negatively impacting law enforcement's ability to conduct electronic surveillance. According to an FBI official, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

Emerging Technologies

Depending on the law enforcement agency, emerging technology impacts their ability to conduct electronic surveillance to varying degrees. A New York law enforcement official stated that the technology is changing at such a high rate of speed that law enforcement needs the FCC to step in. He also noted that "the carriers are doing what the criminals couldn't do – putting law enforcement out of business," by releasing technology without a solution and by charging fees that make electronic surveillance cost prohibitive (this issue is discussed further in Finding IV).

According to law enforcement officials, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED]. A law enforcement official stated that his agency has experienced [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] before the target has changed phones. Therefore, he believes that law enforcement's ability to conduct a wiretap should be tied to the individual, rather than the phone line, to make the process quicker for switching the line that the wiretap is on. Law enforcement officials noted [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] through the carrier. Additionally, targets are able to evade electronic surveillance by using cell phones purchased in Mexico or by traveling into Mexico to place calls, even if the target uses a U.S. carrier. A law enforcement official noted that calls made on cell phones purchased in Mexico or calls initiated in Mexico are not wiretapped because of security concerns related to working with carriers' international divisions.

Of the 82 affirmative responses to the OIG survey, law enforcement officials indicated that the following emerging technologies negatively affect their agencies' ability to conduct electronic surveillance:

Technologies Impacting Law Enforcement

[Chart Not Available Electronically]

Source: Law enforcement responses to the OIG survey

According to the FBI, Internet "hotspots" such as cyber cafés that provide anonymity with multiple access points, third-party calls using calling cards, and toll free numbers are a "technologically unsolvable problem." These services can only be addressed through investigative techniques, rather than through the application of CALEA. In addition, FBI officials said that commercially available electronic encryption will also hinder law enforcement's ability to collect information from electronic intercepts.⁷⁶ According to the FBI, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

FBI's Plans for Remaining CALEA Funding

About \$45 million in CALEA funds remain for the implementation of CALEA-compliant solutions. As previously discussed, the FBI is negotiating reimbursement agreements with two carriers for the cost of deploying CALEA solutions on their pre-1995 equipment. The funds remaining upon completion of negotiations with the two carriers will be used to reimburse second-tier carriers (e.g., large independent carriers and competitive local exchange carriers serving smaller metropolitan areas such as Cincinnati Bell and Alltel). The FBI expects to exhaust the remaining CALEA funds reimbursing second-tier carriers.

We are concerned about how the FBI plans to use the remaining \$45 million. We recognize that CALEA permits the FBI to reimburse carriers for all reasonable costs associated with bringing pre-1995 equipment, facilities, and services into compliance. Nevertheless, because CALEA implementation was delayed, and because technology has significantly changed from the time of CALEA's enactment, we believe the FBI should reexamine the future benefits of activating CALEA software solutions on wireline systems before expending any additional funding. The basis for our concern revolves around: (1) the growing popularity in Internet telephony, (2) the limited number of intercepts performed on wireline equipment, (3) the apparent limited effect on criminal investigations, and (4) the discussion on emerging technologies. Our conclusion in this area is not only limited to the above discussion, but is also based on the costs of the equipment needed to obtain CALEA-covered wiretaps, the wiretap fees charged by carriers, and the delivery method (as discussed in Finding IV).

Although this list is not all-inclusive, the FBI should consider the following factors prior to expending the remaining \$45 million in CALEA funding:

- law enforcement's priorities as they pertain to emerging technologies;
- the number of intercepts conducted under Title III and FISA;
- the number of CALEA-covered intercepts conducted in prior years and the number expected to be performed in the future;
- the ability of law enforcement in the coverage area to equip a wireroom and pay for the intercept;
- the length of time needed to negotiate with carriers, and for carriers to deploy and activate the software;
- the carriers' schedule for replacing or significantly upgrading their pre-1995 equipment, facilities, or services;⁷⁷ and
- the delivery method the carrier will require law enforcement to accept.

Conclusion

As technology advances at an ever-increasing pace, law enforcement officials must be prepared to deal with emerging technologies. For example, [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].

When considering the changing dynamics of the telecommunications industry, the limited number of CALEA-covered wiretaps reported by four carriers in

11/20/2008

OIG Audit Report 06-13

high-priority locations, and the fact that almost 90 percent of authorized wiretaps are conducted on portable devices, we believe the FBI should consider alternative uses for the remaining CALEA funds.

Recommendations

We recommend that the FBI:

2. Expand the audience of state and local law enforcement representatives participating in its Law Enforcement Technical Forums and the FBI Threat Assessment Surveys. This would allow for a more comprehensive understanding of the electronic surveillance threats to law enforcement.
3. Improve the methodology used to gather accurate and current data regarding the adverse impact on criminal investigations arising from carriers' inability to provide CALEA-compliant wiretaps or access to call-identifying information. This can be accomplished by soliciting detailed information on adverse responses to the Threat Assessment Survey, and through the CALEA helpdesk.
4. Reexamine the benefits of activating CALEA solutions on wireline systems prior to the expenditure of the remaining \$45 million in CALEA funding.

IV. ISSUES REQUIRING RESOLUTION

The development, deployment, and maintenance costs associated with implementing CALEA and who should bear those costs continue to be controversial issues. The 10 carrier officials we interviewed believed that these significant costs will hinder full CALEA-compliance. For law enforcement, electronic surveillance is expensive, and includes wiretap fees charged by carriers, equipment costs, and costs associated with the delivery method. In addition to these costs, law enforcement's ability to conduct electronic surveillance is also hampered by poor customer service by carriers, and the FBI's ability to provide assistance and training on electronic surveillance to state and local law enforcement agencies. As technology advances, carrier and law enforcement costs will increase, and their limited assistance could negatively affect law enforcement's ability to conduct electronic surveillance.

Costs Incurred by Carriers

The 10 carrier officials we interviewed indicated that they were committed to complying with CALEA and that they had, or were actively engaged in deploying, CALEA solutions on their networks. However, these same officials advised us that significant costs will hinder full CALEA-compliance. Specifically, carrier representatives stated that the cost to develop, deploy, and maintain electronic surveillance capabilities have been significant, and that these costs are expected to increase as technology advances. The following are just four examples of what the carriers told us:⁷⁸

- A VoIP provider contracted to pay approximately \$100,000 to a trusted third party (TTP) to develop its CALEA solution. In addition, the TTP will charge a monthly fee of \$14,000 to \$15,000 and \$2,000 for each intercept. These amounts do not include the cost of labor for writing code into the software to accommodate the CALEA solution. In addition, officials from this provider discussed with us "opportunity" costs, in that programmers working on CALEA could be developing new features for its customers. Furthermore, the officials were concerned that the government would mandate that every new feature would have to be CALEA-compliant prior to being offered to the public. Such a restriction would cost the company revenue and place them at a disadvantage in comparison to non-U.S. based providers, who do not have to comply with CALEA.
- A wireless carrier stated that it had spent about \$14 million on standards-based voice and data CALEA solutions. These costs were primarily capital and ongoing labor costs, with the bulk of the money going towards developing Personal Communications Services (PCS) voice interception and second-generation packet-mode service. Furthermore, because all of the carrier's equipment is post-1995, the carrier must bear all costs. This carrier also discussed "hidden costs." For example, resources are pulled from revenue-generating projects to work on CALEA projects. In addition, interaction with vendors to develop CALEA solutions and providing technical assistance to law enforcement is very costly.
- Another wireless carrier estimated that it spent about \$40 million to make its network CALEA-compliant. Again, virtually all of this carrier's equipment was post-1995 and, therefore, its costs were not recoverable from the FBI.

We also obtained the costs that some carriers incurred to deploy their CALEA solutions on a "per switch" basis. Specifically, one wireline carrier stated that the company spent nearly \$24,000 per switch to deploy its CALEA solution on 747 switches. Another wireline carrier stated that its CALEA-compliance cost was over \$33,000 per switch on 222 switches. However, the reported carrier costs, both in the aggregate and on a per switch basis, are not comparable because carrier networks vary greatly in size and switch type.

One carrier representative stated that his company believes law enforcement is frustrated by the new communications technology, but does not fully understand the total cost and complexity of obtaining CALEA wiretaps in a wireline and wireless environment. The representative also said that the costs and complexity involved will be exponentially greater with packet mode technology. He further stated that law enforcement wants the CALEA functionality but is largely unaware of the expense and technical impediments to full implementation. This official believed that the problems for law enforcement must be solved before CALEA is implemented on a larger scale.

Costs Incurred by Law Enforcement

From a law enforcement perspective, conducting electronic surveillance is expensive and includes wiretap fees charged by carriers, equipment costs, and costs associated with the delivery method.

Wiretap Fees Charged by Carriers

Law enforcement's biggest complaint regarding CALEA is the relatively high fees charged by carriers to conduct electronic surveillance. A traditional wiretap costs law enforcement approximately \$250. However, a wiretap with CALEA features costs law enforcement approximately \$2,200 according to law enforcement officials and carrier representatives we interviewed. A law enforcement official noted that, "[w]ith CALEA, the carriers do less work but it costs approximately 10 times as much to do a CALEA-compliant tap versus a traditional tap." Law enforcement officials agree that the features provided by CALEA are valuable. However, some law enforcement agencies cannot afford to conduct the number of wiretaps they believe is necessary to support their investigations. We found that other agencies have chosen to conduct traditional wiretaps because of the high carrier fees associated with the CALEA features. In addition, we found that carrier fees varied widely.

During our site visits to federal, state, and local law enforcement agencies, we obtained carrier fee schedules and invoices. The carrier invoices were not itemized, which is a source of contention between law enforcement and the carriers. Law enforcement officials stated that the carriers refuse to provide their agencies with itemized bills that detail the charges for each intercept (i.e., initiation fee, maintenance fee, "pinging" fee, and cost of reports). The agency can verify that the wiretap was active on the dates indicated on the bills, but not what the total cost listed on the bill is based on. Therefore, we were unable to determine if the carriers are passing capital costs on to law enforcement.⁷⁹ However, as previously noted, one carrier informed us that most of the costs it billed to law enforcement are for overtime and recovery of capitalized hardware and software costs. These representatives stated that capital costs are the major costs incurred by a carrier, and that these costs are entirely proper for carriers to recover. These representatives also stated that capital costs will continue to grow as technology accelerates.

One law enforcement official noted that prosecutors are unable to challenge the carriers' costs during the course of the electronic surveillance because <http://www.usdoj.gov/oig/reports/FB...>

11/20/2008

OIG Audit Report 06-13

to do so would be a civil matter and the wiretap orders are sealed by the criminal court. The prosecutor would have to wait until the criminal matter was completed. The law enforcement official stated that at that point the electronic surveillance is no longer needed and the prosecutors do not have time to pursue the issue.

Using the wireless carrier fee schedules provided by law enforcement, we calculated a total base cost per intercept to illustrate the cost variances by carrier for the same type of electronic surveillance and the cost variances charged to different law enforcement agencies by the same carrier.⁸⁰ As depicted in the following tables, we received fee schedules within the same state for four carriers (Carriers A, B, G, and H).

Since some carriers charge a flat fee while others charge an initiation fee plus a daily maintenance fee, we based our calculations for pen register fees on a 60-day period and Title III wiretap fees on a 30-day period since that is the timeframe covered in court orders. In addition to the base calculation provided in the tables, additional fees may be charged by the carriers including monthly maintenance fees, per switch set-up fees, additional switch fees, uninterrupted continuation fees, call-bridging fees, extension fees, and fees for activity reports.

| BASE FEE FOR A 60-DAY PEN REGISTER (WIRELESS) | | | | | |
|---|---------|---------|---------|---------|---------|
| | NY | FL | AZ | CA | NV |
| CARRIER A | \$1,775 | | | \$1,775 | \$1,775 |
| | | | | \$2,600 | \$2,200 |
| CARRIER B | | | \$1,775 | \$1,775 | \$600 |
| | | | | \$2,075 | |
| | | | | \$2,600 | |
| CARRIER C | | \$1,400 | | | |
| CARRIER D | | | | \$600 | \$1,200 |
| CARRIER E (Telephone) | \$1,750 | \$1,750 | \$1,750 | \$1,750 | |
| CARRIER E (Push-To-Talk) | \$2,000 | \$2,000 | \$2,000 | \$2,000 | |
| CARRIER F | | | \$1,750 | \$1,750 | \$1,750 |
| CARRIER G | \$350 | | | \$250 | \$400 |
| | | | | \$350 | \$450 |
| | | | | \$3,100 | |
| CARRIER H (New Order) | \$1,135 | | \$1,135 | \$1,025 | \$1,135 |
| | | | | \$1,135 | |
| CARRIER H (Renewal) | \$820 | | \$820 | \$820 | \$820 |
| CARRIER I | \$350 | | | | |
| CARRIER J | | | | | \$250 |

Source: Carrier fee schedules provided by individual law enforcement agencies

| BASE FEE FOR A 30-DAY TITLE III (WIRELESS) | | | | | |
|--|---------|---------|---------|---------|---------|
| | NY | FL | AZ | CA | NV |
| CARRIER A | \$1,775 | | | \$1,775 | \$1,775 |
| | | | | \$2,600 | \$2,200 |
| CARRIER B | | | \$1,775 | \$1,775 | \$600 |
| | | | | \$2,600 | |
| | | | | | |
| CARRIER C | | \$1,600 | | | |
| CARRIER D | | | | \$600 | \$1,200 |
| CARRIER E (Telephone) | \$1,750 | \$1,750 | \$1,750 | \$1,750 | |
| CARRIER E (Push-To-Talk) | \$2,000 | \$2,000 | \$2,000 | \$2,000 | |
| CARRIER F | | | \$1,000 | \$1,000 | \$1,000 |
| CARRIER G | \$350 | | | \$100 | \$350 |
| | | | | \$350 | \$400 |
| | | | | \$3,100 | |
| CARRIER H (New Order) | \$940 | | \$940 | \$575 | \$940 |
| | | | | \$940 | |
| CARRIER H (Renewal) | \$675 | | \$675 | \$675 | \$675 |
| CARRIER I | \$350 | | | | |
| CARRIER J | | | | | \$250 |

11/20/2008

OIG Audit Report 06-13

Source: Carrier fee schedules provided by individual law enforcement agencies

The above fee calculations illustrate that carriers' fees range from \$250 to \$3,100 to conduct pen registers and Title III wiretaps. Carrier fees are also inconsistent among law enforcement agencies and states. For instance, Carrier B charges a Nevada law enforcement agency \$600 for a Title III wiretap while the same carrier charges a California law enforcement agency \$1,775 and another California law enforcement agency \$2,600.

The cost to conduct electronic surveillance for one case can quickly rise. For example, if law enforcement needs to conduct electronic surveillance beyond the 30- and 60-day timeframes, a new court order requesting an extension must be obtained and, in most cases, the law enforcement agencies are charged the same fees again by the carriers. In addition if another target is identified during the monitoring of the initial target, another court order is obtained to initiate an additional wiretap. A law enforcement official stated that a typical case for his agency usually involves five to six targets. If a target uses more than one phone, the cost to law enforcement rises proportionately.

From the 82 responses to our survey from law enforcement officials indicating that their agency conducts electronic surveillance, 31 agencies (38 percent) indicated that the number of intercepts conducted is hindered by the costs charged by carriers.

In its March 2004 *Joint Petition*, DOJ requested that the FCC:

1. confirm that carriers bear sole financial responsibility for CALEA implementation costs for post-January 1, 1995, communications equipment, facilities and services;
2. permit carriers to recover their CALEA implementation costs from their customers; and
3. clarify the cost methodology and financial responsibility associated with intercept provisioning.

In its NPRM, the FCC sought comment on:

- Cost recovery options that could reduce CALEA-related burdens otherwise imposed on carriers and their customers, including options that more equitably spread costs among the general public. For example, the FCC questioned whether CALEA costs should be recovered directly from consumers by means of an FCC-mandated, flat monthly charge; and
- Whether the FCC should distinguish carrier recovery of CALEA incurred capital costs generally from recovery of specific intercept-related costs. In addition, the FCC sought comment on the costs that can be included in intercept provisioning costs and the entities that should bear financial responsibility for those costs.

Equipment Costs

In order to conduct CALEA wiretaps, law enforcement agencies must maintain or have access to a wireroom. A wireroom consists of a computerized system that intercepts, decodes, records, and plays back telephone communications. The installation of these facilities is both time-consuming if not already in place (it must be ordered weeks or months in advance) and expensive. Depending upon the number of wiretaps conducted and available funding, law enforcement agencies may elect to maintain their own wireroom, maintain a wireroom in conjunction with another agency, or request the temporary use of a wireroom maintained by another agency. Although law enforcement officials noted that their wirerooms are also available for use by other law enforcement agencies in their general vicinity, the smaller law enforcement agencies are limited in conducting electronic surveillance due to the fees charged by carriers.

Of the 82 responses to our survey from law enforcement officials indicating that their agency conducts electronic surveillance, 48 agencies (59 percent) maintain their own wireroom. Law enforcement officials representing the 82 agencies indicated that the number of intercepts conducted by their agencies is hindered by the cost to purchase equipment (16 of 82 responses) and the cost of equipment maintenance (11 of 82 responses).

According to law enforcement officials we interviewed and those who responded to our survey, law enforcement agencies have spent between hundreds of thousands to several million dollars to equip their wirerooms. The equipment costs depend upon the desired capacity of simultaneous wiretaps and the need to accommodate the carriers' various delivery methods (as discussed in the following section). A typical wireroom, as pictured below, consists of the following equipment:

- Monitor and playback stations (PCs)
- Servers (the number of servers required is dictated by the carrier's delivery method)
- An audio recorder (known as a jukebox) which saves the data on a magnetic drive
- Routers (the number of routers required is dictated by the carrier's delivery method)
- A system administration computer



Source: SyTech brochure (permission granted)

11/20/2008

OIG Audit Report 06-13

As an example, the equipment listed below was located in one of the wirerooms that we visited. This particular wireroom has the capacity to conduct eight regular wiretaps or four [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] wiretaps simultaneously.

- 8 computer workstations;
- 3 servers (one to conduct regular cell phone intercepts, one to conduct [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] intercepts, and one to conduct pager and Internet intercepts);
- 1 jukebox, which saves the data on a magnetic drive;
- 1 separate router for [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED] intercepts (all other carriers are on a Virtual Private Network (VPN)); and
- 1 computer monitor to switch between the 3 servers.

In addition to the initial purchase of equipment, law enforcement agencies also pay approximately \$30,000 per year in maintenance fees to their equipment vendor. Law enforcement agencies said they spend additional funds for hardware and software upgrades to keep up with improvements and emerging technology.

Equipment costs for collecting the large amount of data will continue to be a major impediment for law enforcement. As technology changes and electronic surveillance becomes more complex, law enforcement will need to carefully consider how they will receive large volumes of data, especially with broadband intercepts. The collection equipment required by law enforcement will be more complex and costly, and law enforcement will also need to develop the technical expertise to operate the equipment.

Delivery Methods

During our site visits, many law enforcement officials noted that CALEA addresses what carriers need to provide to law enforcement agencies without addressing how data is delivered. For example, CALEA does not address whether carriers can use digital or audio phone lines to deliver the audio portions of intercepts. As a result, the delivery method of intercepted data varies by carrier. Due to the various delivery methods, law enforcement agencies must purchase additional equipment to receive the intercepted data from a carrier. The four delivery methods are dial-out, VPN, frame relay, and T-1 lines.

Dial-out. A dial-out solution takes advantage of the PSTN already in place between the carrier equipment performing an intercept and a law enforcement collection site. A dial-out solution only requires a regular telephone line.

VPN. For VPN, carriers use a "secure tunnel" VPN to conduct electronic surveillance over the Internet. The VPN secure tunnel method uses law enforcement's existing connectivity to the Internet to connect to a specific point in the carrier's network. Firewalls and encryption keys are used to authenticate the law enforcement agency before any intercepted call-identifying information or content is delivered from the carrier's network. This method keeps the information secure when traversing the Internet, and does not require the law enforcement agency's connection to the Internet to be dedicated to a specific carrier or to receiving CALEA information. The best features of a VPN-type connection are that the law enforcement agency can use the same connection to the Internet for multiple applications such as web browsing, e-mail, and CALEA connectivity.

Frame Relay. A frame relay connection consists of three parts: (1) the connection from the law enforcement agency to the carrier's frame relay, which is a private, specific-use circuit that connects a single law enforcement agency location to the carrier's network. This represents the maximum rate at which a law enforcement agency can accept packets from a carrier; (2) the frame relay, which is a network of routers that allow communication from point-to-point without having a dedicated circuit end-to-end; and (3) the connection from the frame relay, which is a private, specific-use circuit that connects multiple law enforcement agencies to the carrier's network. The value of the frame relay connection is its ability to handle large amounts of data, up to the bandwidth of the connection facility, but still not have to pay for that bandwidth point-to-point.

T-1 Line. A T-1 line is a higher capacity circuit using a fiber optic or copper line. A T-1 line can carry 24 digitized voice channels and about 192,000 bytes per second – roughly 60 times more data than a normal residential modem. It is also much more reliable than an analog modem.

One law enforcement official we interviewed stated that he would like to see DOJ mandate the dial-out solution as the delivery method because it is less expensive. A carrier official stated that with dial-out, the line can be connected in two or three days and only costs \$60 per line. However, carriers also noted that not all of the CALEA features are available when dial-out is used because the "pipe" is not large enough for the data stream. Although dial-out is a viable option for receiving call-identifying information and call-content for circuit-mode calls, it may not be a viable option for packet-mode calls. This is because the low connection speed of the dial-out delivery method may not be able to handle the delivery of intercepted packets for law enforcement agencies that handle multiple simultaneous surveillances.

While dial-out and VPN are increasing in popularity, and favored among law enforcement agencies, some carriers only deliver data via a T-1 line. For some law enforcement agencies, T-1 line delivery for a wireline CALEA intercept is impractical. A T-1 line costs law enforcement agencies approximately \$1,300 for installation, and can take up to two months to install. One law enforcement official told us that his agency pays carriers approximately \$20,000 per month to maintain its T-1 connections. He explained that the agency pays \$575 to \$1,800 per month for each circuit.⁸¹

A law enforcement official in California stated that his office was informed by two in-state wireline carriers that they are CALEA-compliant but law enforcement would need to build a T-1 line to each of the carriers' switches. The law enforcement official explained that this concept is unreasonable considering his agency's jurisdiction has about 95 switches from one carrier and about 130 switches from the other. Therefore, it would cost his agency about \$292,500 to install T-1 lines to each of the switches.⁸² This scenario would not be cost beneficial to his agency because a T-1 line is only used for wireline intercepts, and approximately 70 percent of this agency's wiretaps are performed on wireless phones. The law enforcement official stated that there are numerous agencies in California with authority to conduct intercepts and each agency would be required to install a T-1 line to each of the carriers' switches to conduct a CALEA intercept. Another law enforcement official in California estimated that 99 percent of their wiretaps are performed on wireless phones.⁸³ Furthermore, a law enforcement official in Florida also experienced the same situation with one of the carriers noted above. Due to the prohibitive cost of wireline carrier's CALEA solution, the California and Florida law enforcement agencies conduct traditional wiretaps that could not take advantage of CALEA features.

Law Enforcement Assistance Concerns

In addition to monetary issues that affect carriers and law enforcement, we identified assistance concerns that will also affect the successful implementation of CALEA.

Limited Carrier Customer Service

Several law enforcement officials stated that they received poor customer service from the carriers, and believe some carrier employees lack training on initiating and maintaining a CALEA wiretap. In particular, carriers were criticized for bringing down intercepts by upgrading their switches in the middle of the night without notifying law enforcement. In addition, west coast law enforcement officials stated that carriers do not provide customer service after 5:00 p.m. EST. One law enforcement official said that many of the carriers' representatives "have no clue" what law enforcement is talking about when they call with a problem and that he does not think they care or are encouraged to care about law enforcement's problems. Another law enforcement official offered examples when the carrier's switches were able to conduct the intercepts but the carrier's technician did not know how to activate the switches. In addition, law enforcement cited problems with carriers being unable to see the data being sent to law enforcement's monitors until hours

11/20/2008

OIG Audit Report 06-13

later. Although law enforcement receives real-time information, the carriers' service representatives receive the same data hours later, which hinders the carriers' service representatives from providing timely assistance.

Of the 82 affirmative responses to our survey, law enforcement officials indicated the following problems with carriers:

Carrier Problems Experienced by Law Enforcement

[Chart Not Available Electronically]

Source: Law enforcement responses to the OIG survey

Meanwhile a carrier representative told us that most law enforcement agencies blame the carrier if something goes wrong with the intercept. The representative stated that when a law enforcement agency calls with a collection problem, the carrier will deliver the intercept data to its own collection equipment to determine if any problems exist with the delivery of the intercept. When the carrier investigates complaints, about 50 percent of the time it refers the law enforcement agency to the equipment vendor because the problems can be traced to a lack of technical expertise of the law enforcement agency in operating the collection equipment rather than the carrier's lack of customer service.

FBI Support of State and Local Law Enforcement

State and local law enforcement officials indicated that they feel disconnected and unsupported by the FBI on the issue of electronic surveillance. These officials believe that the FBI should provide basic training facilities for law enforcement agents and technical personnel to receive hands-on training on how to conduct CALEA intercepts. During our site visits, we met with state and local wireroom technical agents who were trained as law enforcement officers, but had no prior electronic surveillance experience. However, they were tasked with setting up a wireroom for their agencies, which included dealing with equipment vendors and learning how to conduct electronic surveillance. We believe that state and local agents' learning curves could be reduced dramatically if the FBI provided training. However, the FBI stated they may be limited by Attorney General Order 1945-95 (see footnote number 60) in the level of assistance and training they can provide.

Law enforcement officials who attended the FBI-sponsored Law Enforcement Technical Forums noted that the number of the forums has declined over the last few years. Additionally, we were told that forums have become one-sided with the FBI simply presenting information, instead of an exchange of ideas between the FBI and law enforcement. Law enforcement officials also noted that the FBI should provide an opportunity and venue for vendors to showcase their equipment and analytical programs. Law enforcement officials further mentioned they would like a forum to meet with representatives from the telecommunications carriers in order to voice their concerns. We discussed with the FBI the possibility of the vendors and carriers attending the Law Enforcement Technical Forums. However, FBI officials disagreed with this suggestion, citing security concerns with vendor and carrier personnel.

Our audit also found that some of the state and local law enforcement officials we interviewed were unaware of the resources available to them through the FBI, such as the FBI's CALEA website or its help desk. If law enforcement agencies are unaware of the CALEA website then they are unable to request membership in the Law Enforcement Technical Forum. Members receive invitations to the Law Enforcement Technical Forums where law enforcement representatives can discuss their issues and concerns as well as participate in the Threat Assessment Surveys.

Of the 82 affirmative responses to our survey, 42 (51 percent) law enforcement officials (mostly from the FBI) indicated that their agency had contacted the FBI's CALEA Implementation Unit (CIU) or Engineering Research Facility (ERF) for assistance.⁸⁴ All of the agencies that had contact with the CIU or ERF were satisfied with the assistance provided. The 42 officials noted that the FBI provided ad hoc solutions, software, hardware, and training to their respective agency, as shown in the table below:

Assistance Received from FBI

[Chart Not Available Electronically]

Source: Law enforcement responses to the OIG survey

Conclusion

Law enforcement officials uniformly believe that electronic surveillance is a vital investigative tool and that the CALEA features are extremely beneficial. However, law enforcement agencies are hindered in their ability to conduct the desired number of wiretaps by the cost-prohibitive delivery path offered by some carriers as well as the intercept fees charged by carriers and the costs to set up and maintain a wireroom. While a carrier may be considered CALEA-compliant, it is of no use to law enforcement if the agency cannot afford the delivery path to receive the intercepted data or simply cannot afford the intercept fees.

In addition, we found that state and local law enforcement agencies often do not have the necessary resources to conduct effective electronic surveillance. As a result, state and local law enforcement officials we interviewed indicated they often feel disconnected and unsupported by the FBI, and would benefit greatly from a closer working relationship with the FBI on these issues.

Law enforcement officials said they have experienced poor customer service from some carriers, further complicating their ability to conduct electronic surveillance. For instance, carriers were criticized for bringing down intercepts by upgrading their switches in the middle of the night without notifying law enforcement. In addition, our survey indicated that law enforcement was not provided the intercept data in a timely manner and that some carriers were unresponsive to requests for assistance.

Recommendations

We recommend that the FBI:

5. Provide training for state and local law enforcement agents and technical personnel on how to conduct CALEA intercepts. In conjunction with this recommendation, the FBI should pursue legal clarification of Attorney General Order 1945-95 from the DOJ.
6. Improve liaison between law enforcement officials and carrier and manufacturer representatives by providing a forum to address electronic surveillance issues. This would enhance carrier customer service and law enforcement officials' technical knowledge.

11/20/2008

OIG Audit Report 06-13

Footnotes

40. A switch is a telephone company device which "makes the connection" when a call is placed. Modern switches are specialized computers.
41. According to the U.S. Congress, Office of Technology Assessment, *Electronic Surveillance in a Digital Age*, the costs of the legislation and differences of opinion about who should bear those costs were highly controversial issues during the time leading up to passage of CALEA. The \$500 million figure was a compromise among widely ranging estimates from the telecommunications industry and law enforcement agencies as to the costs of modifying a carrier's equipment and technology to make it CALEA-compliant. Both the telecommunications industry and law enforcement's estimates were based on assumptions about costs for modifying existing equipment and deploying the technology, but the estimates were generally not based on formal engineering cost analysis.
42. In addition, the FBI incurred costs of about \$93 million to administer the CALEA program. This included over \$77 million in contract costs for the telecommunications technical expertise necessary to administer the program. These administrative costs do not include the significant costs incurred by the FBI to develop "ad hoc solutions" that are used to conduct electronic surveillance on switches where the carrier has not developed CALEA solutions. According to FBI officials, the cost of these ad hoc solutions, which are described in Appendix VIII, exceeded \$40 million.
43. These manufacturers account for over 90 percent of telecommunications equipment lines in the United States. The RTU license agreements specified that the software must pass FBI inspection before being disseminated to carriers. In this regard, the payments and obligations mentioned above include more than \$500,000 for carrier assistance in testing the manufacturer's software.
44. According to the FBI, technical electronic surveillance solutions developed by the telecommunications industry provided a limited set of options regarding transporting intercepted information to law enforcement. Technical electronic surveillance solutions required law enforcement to have in place necessary equipment, facilities, and services to transport intercepted information from a carrier's switching (or delivery) equipment to a collection site. The installation of these facilities (wirerooms) is both time-consuming (if not already in place, they must be ordered weeks or months in advance) and expensive. A "dial-out" solution takes advantage of the PSTN already in place between carrier equipment performing an intercept and a law enforcement collection site, and represented a dramatic departure from then-existing delivery mechanisms. However, as discussed in Finding IV of this report, delivery mechanisms remain an impediment for law enforcement to conducting CALEA wiretaps.
45. A carrier's CALEA compliance is not demonstrated simply by installing the CALEA software on a switch. The software must be activated, engineering and provisioning practices developed, security policies implemented, and in some cases, external hardware must be deployed prior to a carrier being able to facilitate surveillance that utilizes the software.
46. The FBI considers areas with the highest amount of switch intercept activity as high priority. As part of the flexible deployment initiatives, the FBI developed a system to rank the carriers' switches from highest to lowest priority to ensure that the CALEA-compliance of high-priority switches was addressed first.
47. The FBI discontinued FlexD II because of the scarcity of technical standards for packet-mode systems. Technical standards are discussed in more detail in the *Developing Technical Standards* section of Finding II.
48. As discussed in the *Carrier Extensions and Enforcement Orders for Non-Compliance* section of Finding II, the FBI advised Verizon, BellSouth, and SBC that it would not support their petitions to the FCC under FlexD III because of their refusal to accommodate law enforcement's high-priority electronic surveillance needs.
49. The FCC has not ruled on these petitions, even though the FlexD III extensions expired in June 2004.
50. Carrier names are omitted to protect proprietary information.
51. These wireless carriers merged; therefore, this table presents their combined results.
52. The J-Standard is the industry published standard to meet the electronic surveillance capability requirements of CALEA. It is discussed in detail in the *Developing Technical Standards* section of Finding II.
53. Prior to issuance of the ESI, the FBI had issued electronic surveillance capabilities in both 1994 (prior to the enactment of CALEA) and 1995. These documents contained the punchlist capabilities.
54. According to the June 13, 2002, *Petition for Further Extensions of Time of CALEA Deadlines* filed on behalf of Qwest Corporation; Malheur Home Telephone Company; Qwest Wireless, LLC; and TW Wireless, LLC; the "core" J-Standard provided law enforcement approximately 95 percent of the capabilities required by CALEA.
55. The nine punchlist capabilities are to: (1) provide the content of subject-initiated conference calls supported by the subject's service, (2) identify the active parties of a multi party call, (3) provide access to all dialing and signaling information available from the subject including a subject's use of features (e.g., the use of flash-hook and other feature keys), (4) notify the law enforcement agency when a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy), (5) provide timing information to correlate call-identifying information with the call content of a communications interception, (6) provide digits dialed by the subject after the initial call "cut-through" is completed to another carrier, (7) send a message to a law enforcement agency that an interception is still functioning on a subject, (8) alert the law enforcement agency via electronic continuity check tone if the facility used for delivery of call content has failed or lost continuity, and (9) notify the law enforcement agency if the subject modifies his subscribed features.
56. The FCC ruled that carriers must comply with punchlist items 1 through 6 identified in footnote 55 and described in more detail in Appendix IX.
57. According to the FBI, the PSFN document neither addressed any procedures for enabling access to a subject's communications nor requirements for how call-identifying information is accessed in a service provider's network. Rather, the document provided a set of high-level needs considered necessary by law enforcement regardless of the service being offered by the provider over a packet-based network. The PSFN Document did recognize that each packet-based service would require a more detailed set of needs based on the specifics of the service and architecture.
58. According to the FBI, this document defined what communications identifying information and communications content are needed by law enforcement to conduct electronic surveillance, but did not define how a service provider should access that information. CGVoP service can be defined as the utilization of packet technology to offer voice services that parallel the services provided through the PSTN and that strive to achieve quality, reliability, security, and connectivity comparable to the PSTN.
59. Personal communication has traditionally been carried via wireline circuits. Advances in computer hardware and software technology have enabled personal communications to be carried via data packets over a network. This method of communication requires both access to a public IP network (e.g., the Internet) and accompanying network infrastructure support services. Network access can be attained from a PIPNAS provider and the necessary network support services can be provided by a PIPNAS provider, application service provider, local exchange carrier, wireless service provider, or some combination thereof.

11/20/2008

OIG Audit Report 06-13

60. Attorney General Order 1945-95 states in part: "It is the policy of the Department of Justice that the loans of electronic surveillance equipment to state and local law enforcement agencies are generally to be discouraged...." The order also states that a "State agency receiving loaned equipment may not disclose the existence or use of such equipment without authority of the FBI Director...." According to the FBI, state and local recipients of FBI ad hoc solutions cannot always protect the details of this sensitive law enforcement technique against subsequent criminal discovery.
61. CALEA solutions are developed by engineers who rely on telecommunications industry published standards to guide them. According to an FBI official, "[s]ince CALEA standards are intentionally broad, this causes software developers to sometimes incorrectly assume the intent of the standard." Complicating the development process is the fact that a different CALEA solution is needed for every combination of carrier and manufacturer in the telecommunications industry, and that some carriers use different manufacturers for the same equipment in different parts of the country.
62. Telcordia Technologies, Inc. is a provider of telecommunications network software and services for IP, wireline, wireless, and cable companies. CableLabs is a research and development consortium of cable television system operators that conducts and funds research and development projects to help cable companies plan for the future and apply technology to meet consumers' needs.
63. The FBI funded testing of solutions only in connection with the nationwide RTU licenses as a contractual condition and not as a part of a comprehensive testing regimen.
64. In granting a Section 109 extension, the FCC also considers the following factors: (1) the effect on public safety and national security; (2) the effect on rates for basic residential telephone service; (3) the need to protect the privacy and security of communications not authorized to be intercepted; (4) the need to achieve the capability assistance requirements of Section 1002 of this title by cost-effective methods; (5) the effect on the nature and cost of the equipment, facility, or service at issue; (6) the effect on the operation of the equipment, facility, or service at issue; (7) the policy of the United States to encourage the provision of new technologies and services to the public; (8) the financial resources of the telecommunications carrier; (9) the effect on competition in the provision of telecommunications services; (10) the extent to which the design and development of the equipment, facility, or service was initiated before January 1, 1995; and (11) such other factors as the Commission determines are appropriate.
65. 47 U.S.C. § 1002(b).
66. A carrier could defend itself by showing that full wiretap capability was not reasonably achievable in its system, or that law enforcement could obtain the same information elsewhere.
67. CALEA offers additional features not available through a traditional wiretap. These additional features are the "punchlist" features described in Appendix IX.
68. CALEA software is considered deployed when it is activated, engineering and provisioning practices developed, security policies implemented, and in some cases, external hardware is deployed prior to a carrier being able to facilitate surveillance that utilizes the software.
69. The FBI estimates that entering into software activation agreements with these four carriers would make about 90 percent of the wireline switches CALEA-compliant.
70. For a description of the CALEA punchlist features, see Appendix IX.
71. The Omnibus Crime Control and Safe Street Act of 1968 required the Administrative Office of the United States Courts (AO) to report to Congress the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The statute requires that specific information be provided to the AO, including the offense(s) under investigation; the location of the intercept; the cost of the surveillance; and the number of arrests, trials, and convictions that directly result from the surveillance.
72. The FBI acknowledged that over 80 percent of intercepts are conducted on cellular or wireless switches.
73. The FBI formed the Law Enforcement Technical Forum and the Law Enforcement Executive Forum to solicit the technical and programmatic exchange of information with the law enforcement community on CALEA implementation and electronic surveillance challenges.
74. During our audit we noted other discrepancies regarding the collection and tabulation of survey responses that resulted in the FBI reissuing a corrected 2004 Threat Assessment Survey Report.
75. [LAW ENFORCEMENT SENSITIVE INFORMATION REDACTED].
76. Under CALEA, carriers are not responsible for decrypting, or ensuring the government's ability to decrypt any communication encrypted by a customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.
77. According to CALEA, if the FBI has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any equipment, facility, or service deployed on or before January 1, 1995, into compliance with the assistance capability requirements of Section 103, such equipment, facility, or service shall be considered to be in compliance with the assistance capability requirements of Section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification.
78. We present this information because the cost of CALEA compliance remains a controversial issue and a concern for carriers. This information was provided by carrier representatives we interviewed and was not audited.
79. According to DOJ's *Joint Petition*, the FCC should clarify the costs that can be included in intercept provisioning costs and determine who bears financial responsibility for such costs. Although carriers are permitted under Title III to pass on to law enforcement their provisioning costs, a growing number of law enforcement agencies expressed concern over the significant provisioning costs in carriers' bills. These costs make surveillance more difficult, especially for smaller law enforcement agencies. To permit carriers to include their CALEA implementation costs in their provisioning costs would not only violate Title III, but will also make it increasingly cost-prohibitive for law enforcement to conduct intercepts. Although Title III provides for carriers to be compensated for costs associated with intercept provisioning, nothing in either Title III or CALEA authorizes carriers to include CALEA implementation costs in their provisioning costs.
80. Wireline fee schedules were not provided by law enforcement because the majority of intercepts are conducted on wireless phone.
81. Another option is to lease access to the carrier's T-1 lines through the law enforcement agency's equipment vendor. Equipment vendors gain permission from the carrier to place a collection box on the carrier's server through which the vendor receives the intercepted data and subsequently passes the data onto the requesting law enforcement agency. A law enforcement official stated that his agency leases access to the carrier's T-1 line through their vendor at a rate of \$750 per month.
82. Calculation is based on the assumption it would cost \$1,300 per switch for installation.

11/20/2008

OIG Audit Report 06-13

83. The difference between the two agencies' percentage of wiretaps performed on wireless phones was attributed to the types of cases each agency conducts; in particular, more wirelines are wiretapped in homicide cases than in drug cases.
84. After a series of reorganizations, responsibility for CALEA implementation now rests within the FBI's Investigative Technology Division (ITD). Within the ITD, the CIU and ERF are tasked with developing overarching CALEA implementation strategies and developing ad hoc solutions.

[« Prev ous](#)

[Table of Contents](#)

[Next »](#)

Exhibit F

Nextel Communications, Inc.
2001 Edmund Halley Drive, Reston, VA 20191
703 433-4000



May 26, 2000

George B. Quinlan
Deputy Attorney General-In-Charge
State of New York
Office of the Attorney General
Organized Crime Task Force
101 East Post Road
White Plains, NY 10601-5008

Dear Mr. Quinlan:

In response to your letter dated March 30, 2000, I write to clarify Nextel's practice of billing law enforcement agencies when Nextel has assisted with the implementation of electronic surveillance. The *Nextel Communications Subpoena & Court Order Compliance Guide for Law Enforcement* states, "Nextel will seek reimbursement from Law Enforcement for reasonable costs associated with supporting and maintaining electronic surveillance requests on the Nextel wireless network, as authorized through applicable statutes." It is my understanding that you are in possession of this handbook and were aware of our practice prior to requesting assistance from Nextel.

Obviously, you are well aware of the statutes that allow telecommunications carriers to recover these costs from law enforcement agencies. Your concerns are apparently related to the methodology used to develop these costs for Nextel, as well as the associated invoices you have received from Nextel. Nextel invoices law enforcement agencies based on the number of surveillance targets provided by the law enforcement agency and by the number of switches in which the surveillance is requested. Basically, Nextel charges an initial installation fee of \$1250 per surveillance target, per switch. In addition, Nextel charges a monthly maintenance fee of \$250 per surveillance target, per switch.

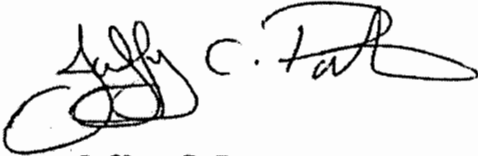
This billing model was created after detailed analysis of the hard dollar costs and associated labor costs to implement and maintain the MAP/CIS solution that gave Nextel the ability to support electronic surveillance, which was a proactive move on the part of Nextel to support requests from law enforcement. Nextel was neither required nor mandated to implement this solution, and the solution itself provided no incremental business benefit to Nextel. The billing model took into account nearly \$2.3 million to implement and maintain the solution in 32 switches. It is important to note that the solution, and actually significant upgrades to the solution, has been installed in nearly twice that number of switches without consideration of an increase in the charges. Nextel also considered the estimated number of electronic surveillance requests that would be processed by Nextel over a three-year period, based on industry electronic surveillance

statistics and projected Nextel market share. My understanding is that this list of charges was presented to representatives at the Department of Justice, and those representatives deemed the charges to be reasonable for the purpose of billing law enforcement agencies for the services rendered to support electronic surveillance.

Nextel has been proactive in continuing to increase and improve the level of support that is offered to law enforcement agencies, and we plan to continue those activities. Nextel spent a significant amount of money in 1999 to upgrade all of our switches to the next generation of intercept tools, and this has also never been factored into the list of charges. We bill for charges associated with providing electronic surveillance support, and we recognize that we will never recoup the expenses associated with providing electronic surveillance capabilities. Although we are reviewing our current billing model, we don't feel that our charges should be compared to the charges levied by other telecommunications carriers who have networks that are different from that of Nextel. Until such time that we amend our billing model, the current charges are applicable for providing electronic surveillance support.

Nextel is committed to assisting law enforcement agencies with their electronic surveillance requests, and we are building a very strong relationship with our law enforcement "customers". Please feel free to contact my team for further support, and we look forward to assisting you in your investigative pursuits.

Sincerely -

A handwritten signature in black ink, appearing to read 'Jeffrey C. Porter', with a stylized flourish at the end.

Jeffrey C. Porter
Director - Technology Security & Fraud

Exhibit G

001-20-2000 00-10 0017
THIS COPY FOR
Mary Kay Albert

2 pages

verizon wireless

Verizon Wireless
180 Washington Valley Rd.
Bodminster, New Jersey 07921

September 25, 2000

Honorable Eliot Spitzer
Attorney General of New York
2nd Floor
Albany, NY 12224

RECEIVED
NY's Office of the Attorney General

SEP 28 2000
Consumer Frauds Bureau
Albany, New York

To Whom It May Concern:

We are requesting your assistance in notifying the law enforcement community of some updates and changes to the process for serving Verizon Wireless with legal process.

We have enclosed updated contact information, a fee schedule, and forms that should accompany the requests.

Your assistance in notifying the law enforcement agencies that you work with would be greatly appreciated.

Sincerely,

Kimberly Brown

Kimberly Brown
Associate Director - Compliance

9/25/00



General Information for serving subpoenas, search warrants and court orders on CellCo Partnership d/b/a Verizon Wireless

The corporate name is: CellCo Partnership d/b/a Verizon Wireless.

The mailing address is: 180 Washington Valley Road
Attn: Custodian of Records
Bedminster, NJ 07921

The contact number is: 908-306-4200 (press "0" after hours for EXIGENT situations)

The group hours are: Mon-Fri 7am-8pm Eastern

The fax number is: 908-659-9594 for subpoenas, search warrants and other legal requests
908-306-4057 for court orders

Please be very specific with your requests and the timeframe for which you need the information. Do not include such wording as "any and all records" as this is much too broad a statement. The courts have traditionally ruled that this wording is considered to be overly broad and overly burdensome. The following information is provided when you ask for:

Subscriber: name and address of the customer
Credit information: social security number and contact numbers of customer
Call details/tolls: date, time of call, number dialed, and the length of call for outgoing calls
Calls to a number: list of calls made to the number
Features: list of the features on the customer's phone

If you need to know what carrier has a certain area code/exchange, please contact 1-800-LAW BUST between 7am to 11pm (EST), 7 days per week. If you have any questions, please call us first to avoid having to reissue a request.

General Fee Schedule¹

| Type of Request | Fee |
|---|---|
| Calls to a number (incoming) within 30 days | \$10.00 per number |
| Calls to a number (incoming) over 30 days | \$100.00 daily per number per switch |
| All mobiles that called a number within 30 days | \$10.00 per number |
| All mobiles that called a number over 30 days | \$100.00 daily per number per switch |
| Bill copies over 90 days or more than 3 months | \$5.00 per copy |
| Electronic Surveillances – new orders | \$125.00 set up per switch, \$15.00 daily per number per switch |
| Electronic Surveillances – renewal orders | \$15.00 daily per number per switch (if the order has expired before the renewal is received it is billed as a new order) |
| SMART (pen registers for Lucent switches only) – new orders | \$30.00 new user set-up (one time only per agency), \$50.00 set up per number, \$10.00 daily per number, \$10.00 for password reset |
| SMART renewals | \$10.00 daily |

¹This fee schedule will be effective October 1, 2000. Billing may be subject to adjustment based on applicable laws. Rates are subject to change.

9/25/00





Subpoenas and Search Warrants

This form is to be completed and a copy of it faxed or mailed with all subpoenas and search warrants served upon CellCo Partnership d/b/a Verizon Wireless.

Contact Information

Agency name: _____

Agency Address: _____

Agent Name: _____

Contact Number: _____

Fax Number: _____

Billing Information

Bill to Name (if different from above): _____

Bill to Address: _____

Billing Contact Name: _____

Contact Number: _____

Fax Number: _____



Court Orders

This form is to be completed and a copy of it faxed or mailed with all court orders served upon CellCo Partnership d/b/a Verizon Wireless.

Contact Information

Agency name: _____

Agency Address: _____

Agent Name: _____

Contact Number: _____

Fax Number: _____

Billing Information

Bill to Name (if different from above): _____

Bill to Address: _____

Billing Contact Name: _____

Contact Number: _____

Fax Number: _____

Set-Up Information

Last 4 digits of targets: _____ Type of equipment: _____

Switch

Line/Binding Post

User login for SMART orders: _____

9/25/00

(LETTERHEAD OF AGENCY)

Verizon Wireless
Attention: Custodian of Records
180 Washington Valley Road
Bedminster, NJ 07921

Dear [name of on-call Specialist]:

This is to confirm my recent telephone conversation with Verizon Wireless. The [named agency] is handling an exigent situation, [provide type of exigent situation; i.e., 911 call], that poses the immediate threat of serious injury to life or property. [Agency] immediately needs the following [description of information – must be detailed and explicit so that Verizon Wireless does not have to guess] that we believe is in Verizon Wireless's possession. [Agency] will provide required legal process (i.e., subpoena, search warrant or court order) covering this request as soon as reasonably possible but no later than any applicable statutory requirement.

[Signature]
[typed name and rank]
[Badge # if applicable]

9/25/00

TOTAL P.05
TOTAL P.06